SOPHOS

# SafeGuard PortProtector 3.30 SP6

## Benutzerhilfe

Stand: März 2010



# Wichtiger Hinweis

Dieses Benutzerhandbuch wird vorbehaltlich folgender Bedingungen und Einschränkungen ausgeliefert:

- Dieses Handbuch enthält Eigentumsinformationen, die Eigentum von Sophos sind. Diese Informationen werden ausschließlich zum Zweck der Unterstützung ausdrücklich und ordnungsgemäß befugter Benutzer von Sophos SafeGuard PortProtector ausgegeben.
- Kein Teil seines Inhalts darf ohne vorherige schriftliche Genehmigung von Sophos für einen anderen Zweck verwendet, anderen Person oder Unternehmen offenbart oder in irgendeiner Weise, elektronisch oder mechanisch, reproduziert werden.
- Text und Grafik dienen ausschließlich der bildhaften Darstellung und Referenz. Änderungen der Angaben, auf welchen sie basieren, bleiben vorbehalten.
- Die in diesem Handbuch beschriebene Software wird unter Lizenz zur Verfügung gestellt. Die Software darf nur in Übereinstimmung mit den Bedingungen dieser Vereinbarung verwendet oder kopiert werden.
- Änderungen der in diesem Handbuch enthaltenen Informationen bleiben vorbehalten. Sofern nichts anderes erwähnt wird, sind die in diesem Dokument verwendeten Namen und Daten von Unternehmen und Einzelpersonen frei erfunden.
- Alle Informationen in diesem Dokument sind nach bestem Wissen und Gewissen gegeben, jedoch ohne jegliche Gewähr auf Genauigkeit, Vollständigkeit oder Sonstiges, und mit dem ausdrücklichen Verständnis, dass Sophos keinerlei Verpflichtungen gegenüber Dritten in irgendeiner Form hat, die aus den Informationen oder im Zusammenhang mit den Informationen oder deren Nutzung entstehen.
- Sophos SafeGuard PortProtector und Sophos SafeGuard PortAuditor sind OEM-Versionen der Safend-Produkte Safend Protector und Safend Auditor. Einige Screenshots in diesem Handbuch weisen daher das Safend-Branding auf, haben jedoch die gleiche Bedeutung und Funktionsweise wie in der SafeGuard OEM-Version.

Boston, USA | Oxford, UK





# Über dieses Handbuch

Dieses Handbuch besteht aus den folgenden Kapiteln:

- ***Kapitel 1, Einführung in SafeGuard PortProtector,*** stellt die SafeGuard PortProtector-Lösung sowie die Architektur des Systems vor und beschreibt, wie es funktioniert. Es beschreibt die Funktionen und Vorteile, insbesondere die neuen Funktionen in dieser Version, und zeigt einen Workflow-Vorschlag, wie das System für den Schutz der Endpunkte in Ihrer Organisation eingesetzt werden kann.
- ***Kapitel 2, Erste Schritte,*** beschreibt, wie die SafeGuard PortProtector Management Console gestartet wird. Danach folgt ein kurzer Überblick über die Benutzeroberfläche der SafeGuard PortProtector Management Console und eine Beschreibung der Home-Welt, die Zugang zu den Hauptfunktionen des Systems bietet.
- ***Kapitel 3, Definieren von Policies,*** beschreibt, wie SafeGuard PortProtector-Policies definiert und verwaltet werden.
- ***Kapitel 4, Verteilen von Policies,*** beschreibt das Deployment der SafeGuard PortProtector-Policies auf den Endpunkten Ihrer Organisation.
- ***Kapitel 5, Anzeigen von Logs,*** beschreibt, wie Sie Ihre Organisation überwachen, indem Sie die Logs einsetzen, die Sie von SafeGuard PortProtector Clients erhalten und die die Endpunkte Ihrer Organisation schützen, und auch die Logs, die Sie von SafeGuard PortProtector Servern erhalten.
- ***Kapitel 6, Verwalten von Clients,*** erläutert, wie Sie den Status der SafeGuard PortProtector Clients anzeigen, die die Endpunkte Ihrer Organisation schützen, und wie Aktionen wie etwa das Hochladen von Policies, Überprüfen der letzten Client-Daten etc. auf diesen Clients ausführen.
- ***Kapitel 7, Administration,*** beschreibt, wie Sie die globalen Administrationseinstellungen in SafeGuard PortProtector definieren.
- ***Kapitel 8, Endbenutzer-Erfahrung,*** beschreibt die im Umgang mit den Schutzeinstellungen durch SafeGuard PortProtector Client (wie beispielsweise Endbenutzer-Meldungen) und die auf dem Client durchführbaren Maßnahmen, wie beispielsweise das Verschlüsseln von Wechselspeichergeräten.
- ***Appendix A – Novell e-Directory Synchronization*** (Englisch)
- ***Appendix B – Supported Device Types*** (Englisch), führt die Gerätemodelle auf, die SafeGuard PortProtector beim Erstellen einer Policy zur Auswahl bietet.
- ***Appendix C – Supported File Types*** (Englisch), führt die Dateitypen und Dateierweiterungen auf, die von der Funktion der Dateitypenkontrolle in SafeGuard PortProtector zur Kontrolle der auf Speichergeräte geschriebene bzw. von Speichergeräten gelesene Dateien unterstützt werden.
- ***Appendix D – CD/DVD Media Scanner*** (Englisch), beschreibt. wie bestimmte CD/DVD-Medien gescannt und mit Fingerprints versehen werden, so dass sie in einer weißen Liste zur Nutzung freigegeben werden können.
- ***Appendix E – Using SafeGuard PortProtector in a HIPAA Regulated Organization*** (Englisch), liefert Anleitungen, wie diese Bedrohungen in einer HIPAA-geregelten Umgebung angegangen werden.
- ***Appendix F – Using SafeGuard PortProtector in a SOX Regulated Organization*** (Englisch), liefert Anleitungen, wie diese Bedrohungen in einer SOX 404-geregelten Umgebung angegangen werden.

- ***Appendix G – Using SafeGuard PortProtector in a PCI Regulated Organization*** (Englisch), liefert Anleitungen, wie diese Bedrohungen in einer PCI DSS-geregelten Umgebung angegangen werden.
- ***Appendix H – Using SafeGuard PortProtector in a FISMA Regulated Organization*** (Englisch), liefert Anleitungen zur Adressierung dieser Bedrohungen in einer FISMA-regulierten Umgebung.

# Inhalt

# 1 Einführung in SafeGuard PortProtector

## Über dieses Kapitel

Dieses Kapitel stellt die SafeGuard PortProtector-Lösung vor, beschreibt ihre Funktionsweise und präsentiert einen Workflow-Vorschlag, der beschreibt, wie Sie das System zum Schutz der Daten in Ihrer Organisation einsetzen können. Es enthält die folgenden Abschnitte:

- Die ***SafeGuard PortProtector Lösung*** beschreibt die Lösung von SafeGuard PortProtector für die unternehmensweite Sicherheit der Endpunkte durch Kontrolle und Überwachung des Zugriffs auf die Ports und Geräte in Ihrem Unternehmen.
- ***SafeGuard-Schutz*** beschreibt, wie SafeGuard PortProtector die Ports schützt und den Zugriff auf die daran angeschlossenen Geräte und Speichergeräte beschränkt.
- ***System Architektur*** beschreibt die Architektur und die Komponenten des Systems.
- ***SafeGuard PortProtector Management Console*** beschreibt die Management Console, die das zentrale Tool zur Definition der Schutzpolicies für die Ports in Ihrer Organisation, zur Anzeige von Logs und zur Verwaltung der SafeGuard PortProtector Clients darstellt.
- ***Durchsetzung der SafeGuard Policy – SafeGuard PortProtector Client*** beschreibt SafeGuard PortProtector Client, der transparent auf den Endpunkten in Ihrer Organisation läuft und die SafeGuard PortProtector-Schutzpolicies auf jedem Computer durchsetzt, auf dem er eingesetzt ist.
- ***Workflow zur Implementierung von SafeGuard PortProtector*** beschreibt den Workflow für die Implementierung und Nutzung von SafeGuard PortProtector.

## 1.1 Die SafeGuard PortProtector Lösung

Zusammen mit SafeGuard PortAuditor (siehe *SafeGuard PortAuditor Benutzerhandbuch*) bietet SafeGuard PortProtector eine umfassende Lösung, die Unternehmen folgende Möglichkeiten bietet: zu erkennen, welche Ports und Geräte in ihrer Organisation genutzt werden (**Sichtbarkeit**), eine Policy festzulegen, die deren Nutzung **kontrolliert** und Daten zu **schützen**.

SafeGuard PortProtector kontrolliert jeden Endpunkt und jedes Gerät in jedem Netz und an jeder Schnittstelle. Das System überwacht den Verkehr in Echtzeit und setzt individuell angepasste, höchst effiziente Sicherheitspolicies auf allen physischen und kabellosen sowie auf allen Speichergeräte-Schnittstellen um.

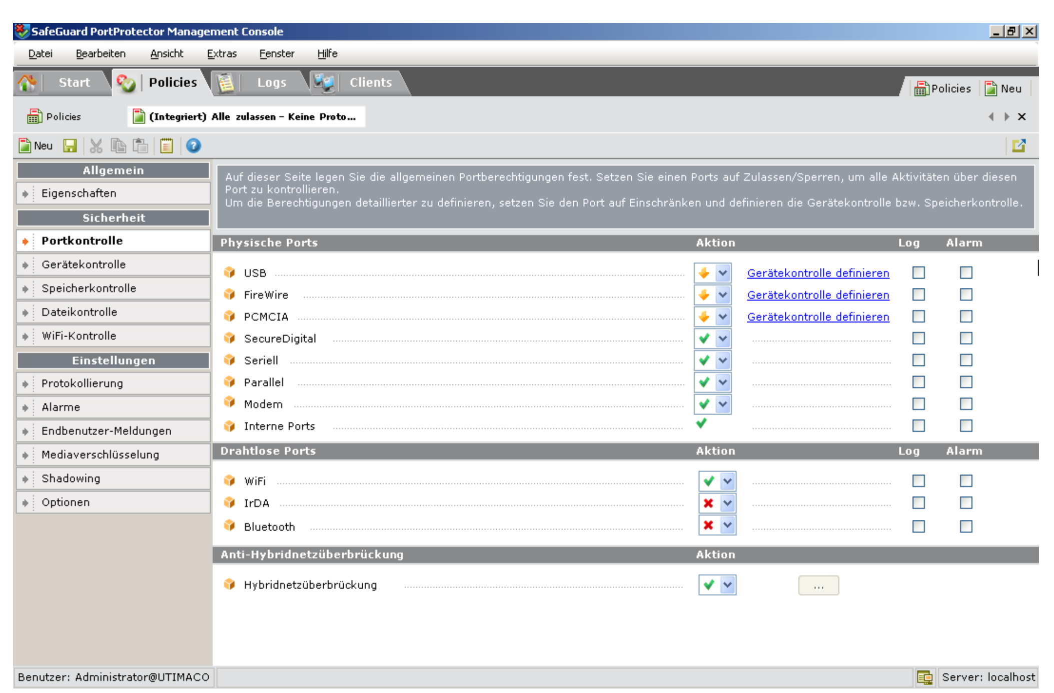
## 1.2 SafeGuard-Schutz

So schützt SafeGuard PortProtector die Endpunkte:

### 1.2.1 Portkontrolle

SafeGuard PortProtector kann die Nutzung beliebiger bzw. aller Computerports in Ihrer Organisation auf intelligente Weise zulassen, sperren oder beschränken, je nach dem auf welchem Computer sich die Ports befinden, welcher Benutzer angemeldet ist und/oder um welchen Porttyp es sich handelt. Safend kontrolliert folgende Ports: USB, PCMCIA, FireWire, Secure Digital, seriell, parallel, Modem (z. B. Einwahl, 3G etc.), WiFi, IrDA und Bluetooth.

Ein gesperrter Port ist nicht verfügbar, so als ob seine Kabel abgetrennt wären. Beim Hochfahren des Computers oder bei der Übernahme einer Policy, die einen zuvor zugelassenen Port sperrt, wird über die Sperrung eines Ports informiert.




Weitere Informationen zur Portkontrolle finden Sie in *Schritt 4: Portkontrolle definieren* im Kapitel *Definieren von Policies*.

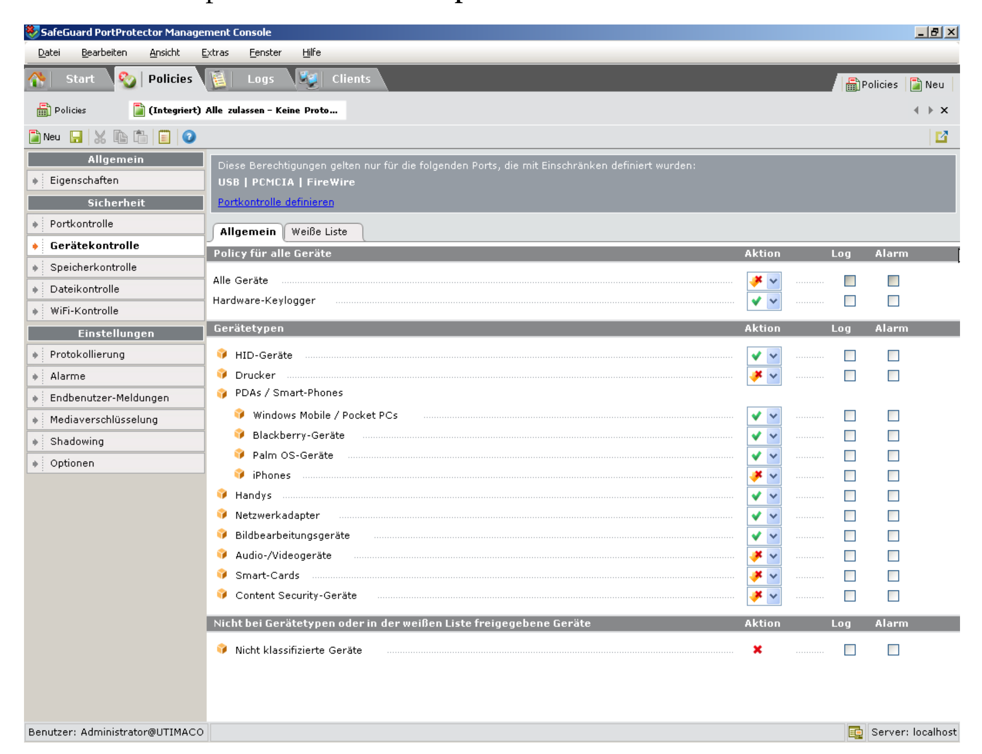
## 1.2.2 Gerätekontrolle

Zusätzlich zur Kontrolle des Portzugangs bietet SafeGuard PortProtector eine weitere Granularitätsstufe: Sie können definieren, welche Geräte auf einen Port zugreifen können.

Für USB-, PCMCIA- und FireWire-Ports können Sie definieren, welche Gerätetypen, Gerätemodelle bzw. welche spezifischen Geräte auf einen Port zugreifen können:

- **Gerätetypen:** Mit dieser Option können Sie den Zugriff auf einen Port je nach Typ des daran angeschlossenen Geräts beschränkten. Zu den Gerätetypen zählen u.a. Drucker, Netzadapter, HID-Geräte (z. B. eine Maus) oder Bildbearbeitungsgeräte.

Die zur Auswahl stehenden Gerätetypen sind in SafeGuard PortProtector integriert. Wenn Sie ein Gerät zulassen möchten, das hier nicht aufgeführt ist, können Sie die nachfolgend beschriebene Option **Modelle** oder **Spezifische Geräte** nutzen.




- **Modelle:** Diese Option bezieht sich auf das Modell eines bestimmten Gerätetyps, wie beispielsweise alle HP-Drucker oder alle M-Systems Disk-on-keys.
- **Spezifische Geräte:** Diese Option bezieht sich auf eine Liste spezifischer Geräte, von denen jedes eine eindeutige Seriennummer hat, wodurch es eigentlich ein spezifisches Gerät ist. Zum Beispiel: Es ist möglich das PDA des CEO zuzulassen und alle anderen PDAs zu sperren.

### 1.2.2.1 Schutz vor Hardware-Keylogger

Hardware-Keylogger sind Geräte, die in feindlicher Absicht von Dritten zwischen eine Tastatur und den zugehörigen Hostcomputer geschaltet wurden, um Tastatureingaben 'abzuhören' und aufzuzeichnen und auf diese Weise kritische Informationen, insbesondere Identifizierungen und Kennwörter, zu stehlen.

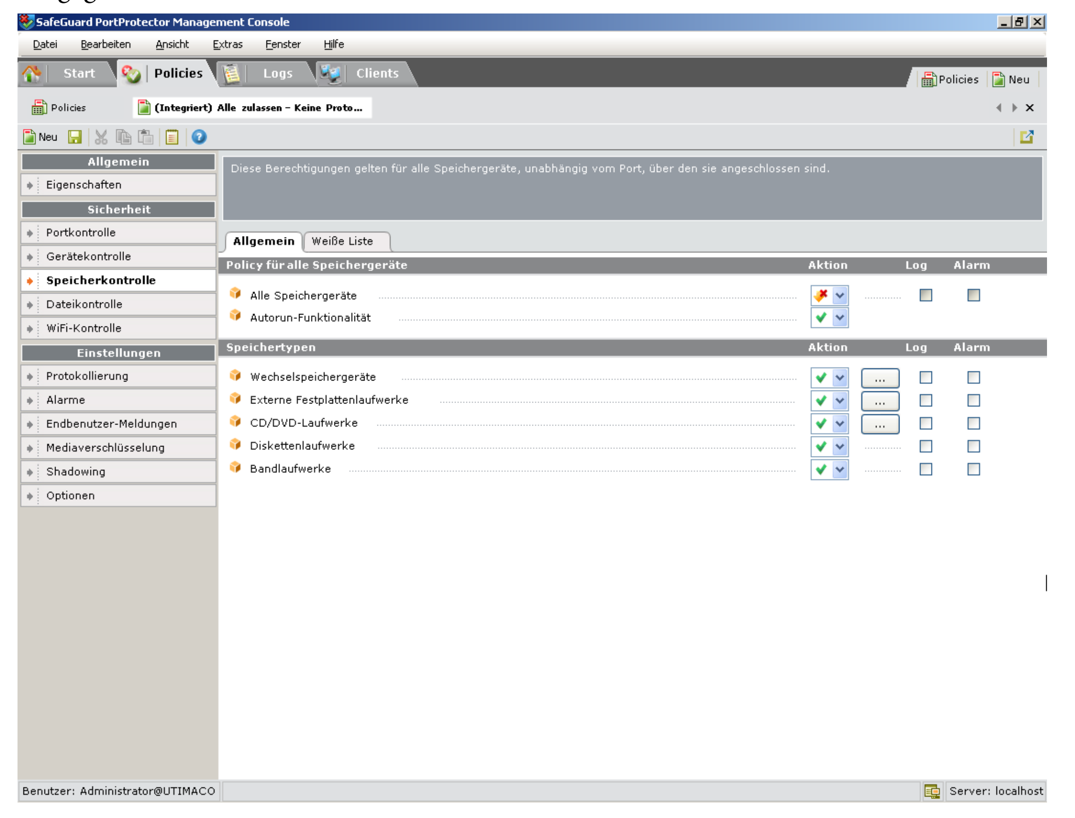
Mit SafeGuard PortProtector können Sie Ihre Benutzer gegen diese Bedrohung schützen: SafeGuard PortProtector kann Hardware-Keylogger erkennen, die an einen USB- oder PS/2-Port angeschlossen sind. Und mit Ihrer Policy können Sie festlegen, ob die Hardware-Keylogger bei Ihrer Erkennung gesperrt werden sollen.

Weitere Informationen zur Gerätekontrolle finden Sie in *Schritt 5: Gerätekontrolle definieren* im Kapitel *Definieren von Policies*.

## 1.2.3 Speicherkontrolle

Die Speicherkontrolle ermöglicht einen weiteren Detaillierungsgrad, in dem Sie die Sicherheitsanforderungen Ihrer Organisation angeben können, die für alle, interne oder externe, feste oder auswechselbare Speichergeräte gelten können. Sie können Speichergeräte komplett sperren und schreibgeschützten Zugriff zulassen. Sie können auch Wechselspeichergeräte verschlüsseln.

Ähnlich wie bei den anderen Geräten, die im vorigen Abschnitt beschriebenen wurden, können Speichergeräte auch abhängig von ihrem Typ, ihrem Modell oder ihrer eindeutigen ID freigegeben werden.



### 1.2.3.1 U3 Smartdrive und Autorun-Kontrolle

Bestimmte Disk-On-Key-Geräte, wie beispielsweise U3-Geräte, bieten neben den grundlegenden Speicherfunktionen eine intelligente Funktionalität. Mit Hilfe dieser Funktionalität können diese Geräte Anwendungen speichern und ausführen, sobald sie an einen Hostcomputer angeschlossen sind.

Mit SafeGuard PortProtector bieten Sie Ihren Anwendern die Möglichkeit, ihre neuen, hochentwickelten Speichergeräte zu nutzen und gleichzeitig sicherzustellen, dass Ihre Endpunkte keiner Gefahr oder risikobehafteten Anwendung ausgesetzt sind, die diese Geräte als Bestandteil ihrer U3- und intelligenten Speichermöglichkeiten mit sich bringen. Sie können ganz einfach sowohl U3-Aktivitäten als auch eine automatische Ausführung im Rahmen Ihrer Sicherheitspolicy sperren. Mit der einzigartigen Client-Technologie von Sophos sind Sie in der Lage, Smart Storage-Geräte als einfache Speichergeräte zu nutzen, solange diese die übrigen Bestimmungen Ihrer Speicherrichtlinie erfüllen, und lediglich Funktionen sperren, die unter Umständen nicht sicher sind.

### 1.2.3.2 SafeGuard PortProtector Speicherverschlüsselung

Mit der SafeGuard PortProtector Speicherverschlüsselung können Administratoren die Verschlüsselung aller Daten erzwingen, die von Endpunkten der Organisation an freigegebene Wechselmediengeräte, wie etwa USB-Flash, Disk-on-Keys, Memorysticks und SD-Karten, sowie CD/DVD- und externe Festplatten übertragen werden.

Einzigartig in der SafeGuard PortProtector-Lösung ist die Möglichkeit, die Nutzung verschlüsselter Geräte und Medien auf Firmencomputer zu beschränken. Dadurch werden die Sicherheitsgrenzen der Organisation erweitert und es wird verhindert, dass Mitarbeiter absichtlich Daten über diese hochleistungsfähigen Geräte durchsickern lassen.

Innerhalb der Organisation ist die Mediaverschlüsselung absolut transparent. Die Endbenutzer können wie gewohnt von den Medien lesen und darauf schreiben. Wenn jedoch dasselbe Gerät oder Medium auf einem Computer eingesetzt wird, der nicht zur Organisation gehört, ist der Zugriff auf die Daten nicht möglich.

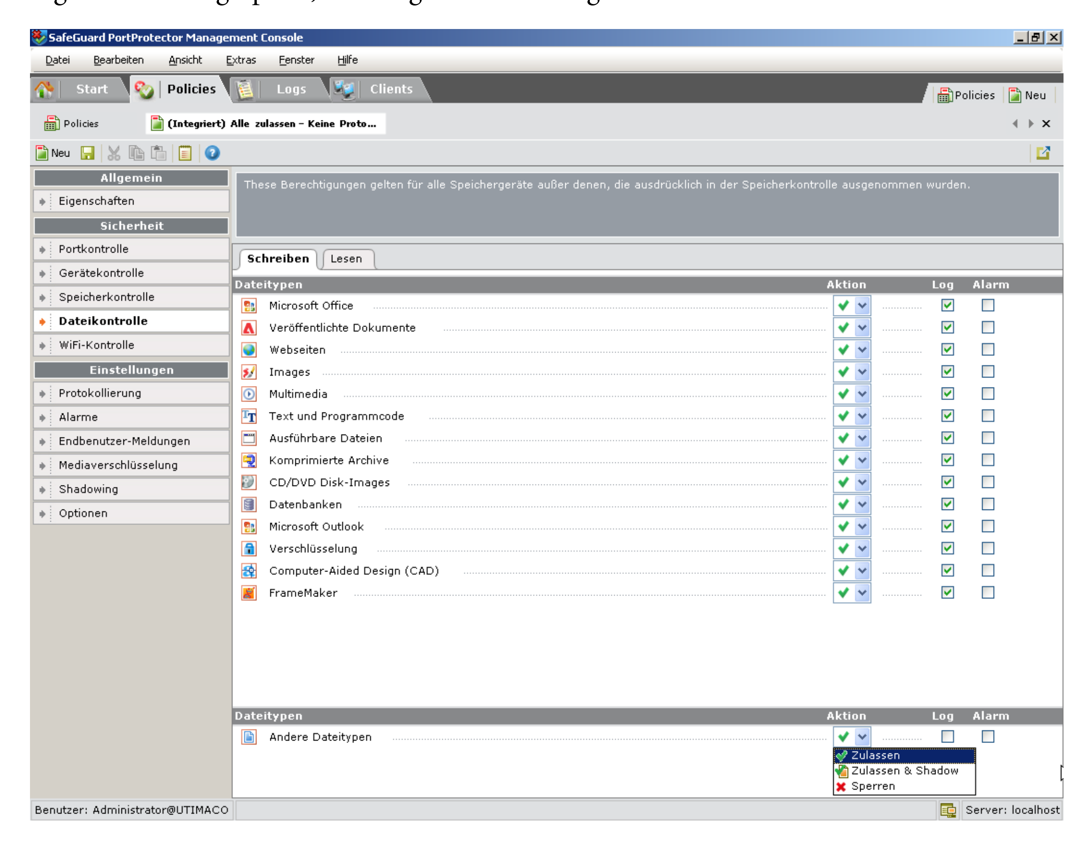
Verschlüsselte Geräte können gelesen und wechselweise auf jedem beliebigen Computer in der Organisation genutzt werden, wobei die Kontrolle auf der Basis von Gerätehersteller/Modell und Seriennummer weiterhin gilt.

Bei Wechselspeichergeräten kann der SafeGuard PortProtector-Administrator angeben, ob bestimmten Benutzern kennwortgeschützter Zugriff auf die Daten auf nicht autorisierten Computern gewährt werden soll. Wird dies erlaubt, kann der Benutzer sein eigenes Offline-Kennwort festlegen und das Offline Access Utility (das sich auf dem verschlüsselten Gerät befindet) auf einem nicht autorisierten Computer benutzen, um für sicheren Zugriff auf die Daten sein Kennwort einzugeben.

Weitere Informationen zur Speicherkontrolle finden Sie in *Schritt* 6: Speicherkontrolle definieren in *Schritt 6: Speicherkontrolle definieren* in *Kapitel 3, Definieren von Policies*.

## 1.2.4 Dateikontrolle

File Control bietet ein weiteres Maß an Granularität und Sicherheit durch die Überwachung und Kontrolle der Dateiübertragung zu/von externen Speichergeräten. Die Definitionen werden auf der Ebene der Dateitypen festgelegt. Dabei können bestimmte Dateiübertragungen zugelassen oder gesperrt, und Logs und Alarme generiert werden.




### 1.2.4.1 Dateitypkontrolle

Mit der Dateitypkontrolle wird eine äußerst zuverlässige Klassifizierung der Dateien durchgeführt, bei der die Inhalte des Datei-Headers anstelle der Dateierweiterung geprüft werden. So wird verhindert, dass Benutzer den Schutz einfach durch Ändern der Dateierweiterung umgehen können. Mit mehr als 180 integrierten Dateierweiterungen, die alle gängigen Anwendungen abdecken und in 14 Dateikategorien eingeordnet sind, wird das Definieren einer Policy einfach wie nie zuvor.

Da sowohl die auf externe Speichergeräte heruntergeladenen als auch auf den geschützten Endpunkt hochgeladenen Dateien geprüft werden, lassen sich mehrere Vorteile erzielen:

- Eine zusätzliche Schutzebene, um das Durchsickern von Daten zu verhindern
- Schutz vor Eindringen von Viren/Schadprogramme über externe Speichergeräte
- Schutz vor Einführung von unsachgemäßen Inhalten über externe Speichergeräte. Beispiele für solche Inhalte sind:
  - Nicht lizenzierte Software
  - Nicht lizenzierte Inhalte (z. B. Musik und Filme)
  - Nicht arbeitsbezogener Inhalt (z. B. persönliche Bilder)

Weitere Informationen finden Sie in *Schritt 7: Dateikontrolle definieren* im Kapitel *Definieren von Policies*.

### 1.2.4.2 Dateiprotokollierung und Shadowing

Die Funktion der Datei-Protokollierung bietet eine weitere Ebene für die Überwachung der Aktivitäten in Ihrer Organisation, mit der Sie die auf Wechselmedien bzw. auf CD/DVD geschriebenen oder davon gelesenen Informationen protokollieren können. Auch Datei-Logs werden in der Logs-Welt angezeigt.

Mit dieser Option erhalten Sie ein Prüfprotokoll darüber, welche Daten in die Organisation bzw. aus ihr heraus transferiert werden. Damit können Sie auch Sicherheitsvorfälle analysieren, die Aktivitäten von Personen nachverfolgen und möglichen Missbrauch tragbarer Speichergeräte erkennen. Auf diese Weise können Sie den Sicherheitsvorschriften, an die Sie möglicherweise gebunden sind, besser entsprechen und die Einsicht in den Datenfluss in Ihrem Unternehmen verbessern.

Für sehr sensible Abteilungen Ihrer Organisation oder für bestimmte Benutzer, die besonderer Aufmerksamkeit bedürfen, können Sie auch die Funktion des Datei-Shadowing einsetzen. Mit dieser Funktion können Sie Kopien der zu/von externen Speichergeräten verschobenen Dateien sammeln. Die Dateien werden in einem zentralen Speicher abgelegt und können von autorisierten Administratoren angezeigt werden. Beachten Sie bitte: Da die Nutzung dieser Funktion sowohl die Netzleistung als auch die Speicherressourcen beeinflusst, sollten Sie sie mit Bedacht – vorzugsweise in kleinen, gut definierten Bereichen Ihrer Organisation – einsetzen.

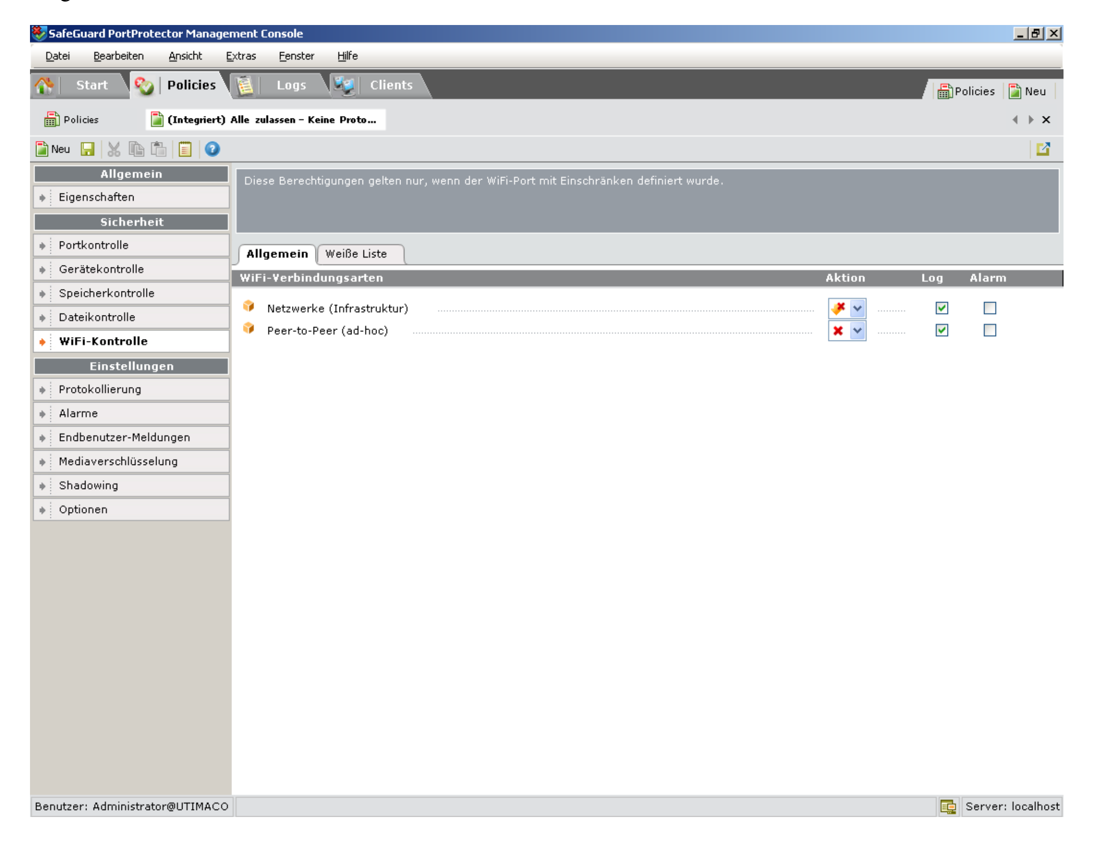
Durch die Überwachung der Dateinamen und das File Shadowing haben Administratoren mehr Flexibilität bei der Erstellung von Policies, die die Nutzung der Geräte nicht einschränken und doch die volle Sichtbarkeit der Aktivitäten und der auf Wechselmedien übertragenen Inhalte zulassen (weitere Informationen finden Sie in *Weitere Berechtigungen* in *Kapitel 3, Definieren von Policies*).

### 1.2.4.3 Integration der Inhaltsprüfung

Die Administratoren können auch von vorhandenen Systemen für die Inhaltsüberwachung und Filterung zur Kontrolle des Dateitransfers auf externe Speichergeräte Gebrauch machen. Bei dieser Technologie kann jede Datei, die von einem Endpunkt auf ein externes Speichergerät heruntergeladen wird, daraufhin überprüft werden, ob sie sensible Informationen enthält (z. B. geistiges Eigentum, Verbraucherdaten etc.). Wenn festgestellt wird, dass die Datei sensible Daten enthält, wird der Benutzer darüber informiert, dass diese Datei nicht auf externe Geräte übertragen werden soll. Zudem wird ein so genanntes Trace-Log für den Administrator erstellt. Dieses Log gibt dem Administrator eine detaillierte Liste der Datenverletzungen durch externe Speichergeräte an die Hand.

## 1.2.5 WiFi-Kontrolle

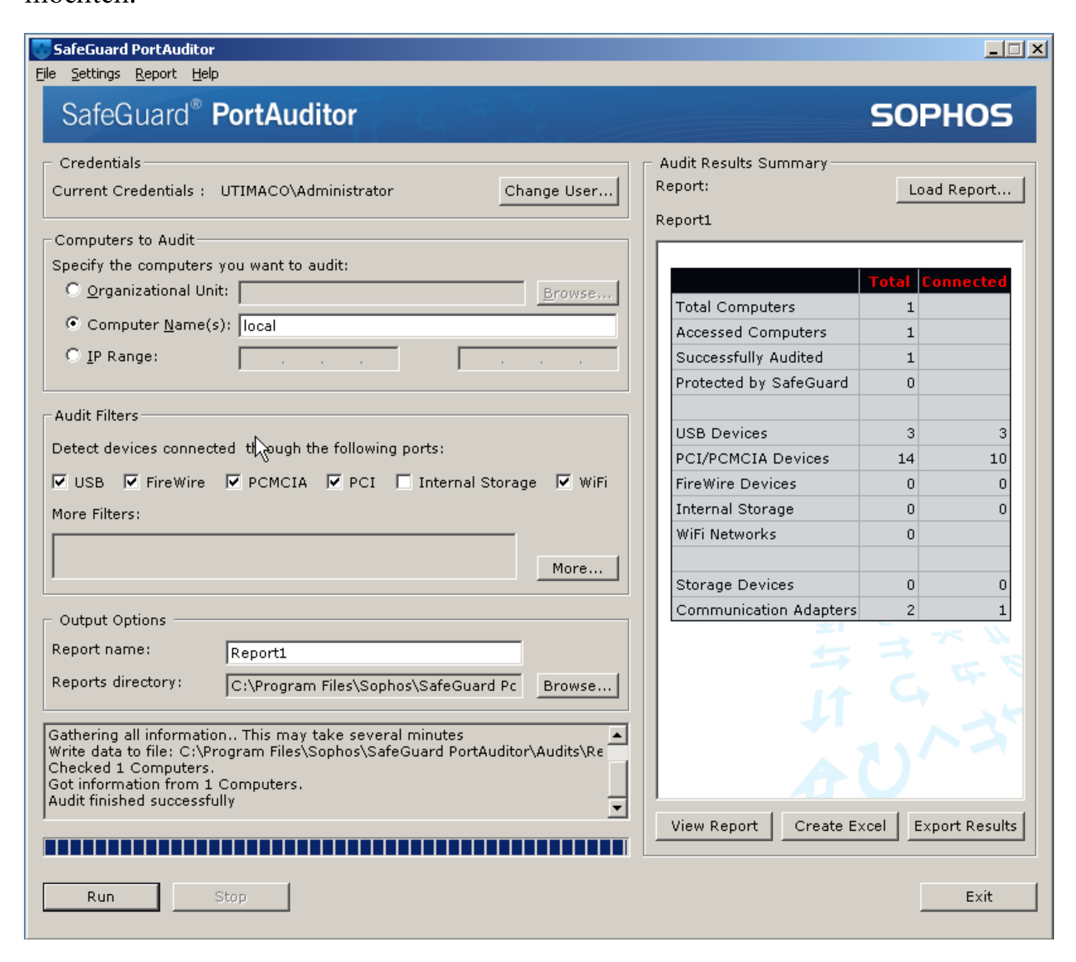
Die WiFi-Kontrolle stellt sicher, dass die Benutzer nur Verbindungen zu zugelassenen Netzen herstellen können. Sie können angeben, welchen Netzen oder Ad-hoc-Links Zugang gewährt wird. Zur Definition der zugelassenen Links können Sie die MAC-Adresse des Zugangspunkts, die SSID des Netzes, die Authentifizierungsmethode und die Verschlüsselungsmethoden angeben.




Weitere Informationen finden Sie in *Kapitel 3, Definieren von Policies*.

### 1.2.5.1 SafeGuard PortAuditor

Auch wenn SafeGuard PortAuditor kein integraler Bestandteil von SafeGuard PortProtector ist, geht dieses Tool doch mit SafeGuard PortProtector Hand in Hand und ergänzt das System mit einer kompletten Sicht darauf, welche Ports, Geräte und Netze von den Benutzern in Ihrer Organisation genutzt werden (oder früher genutzt wurden). Mit Hilfe eines SafeGuard PortAuditor-Scans können Sie die Geräte und Netze auswählen, deren Nutzung Sie zulassen möchten.

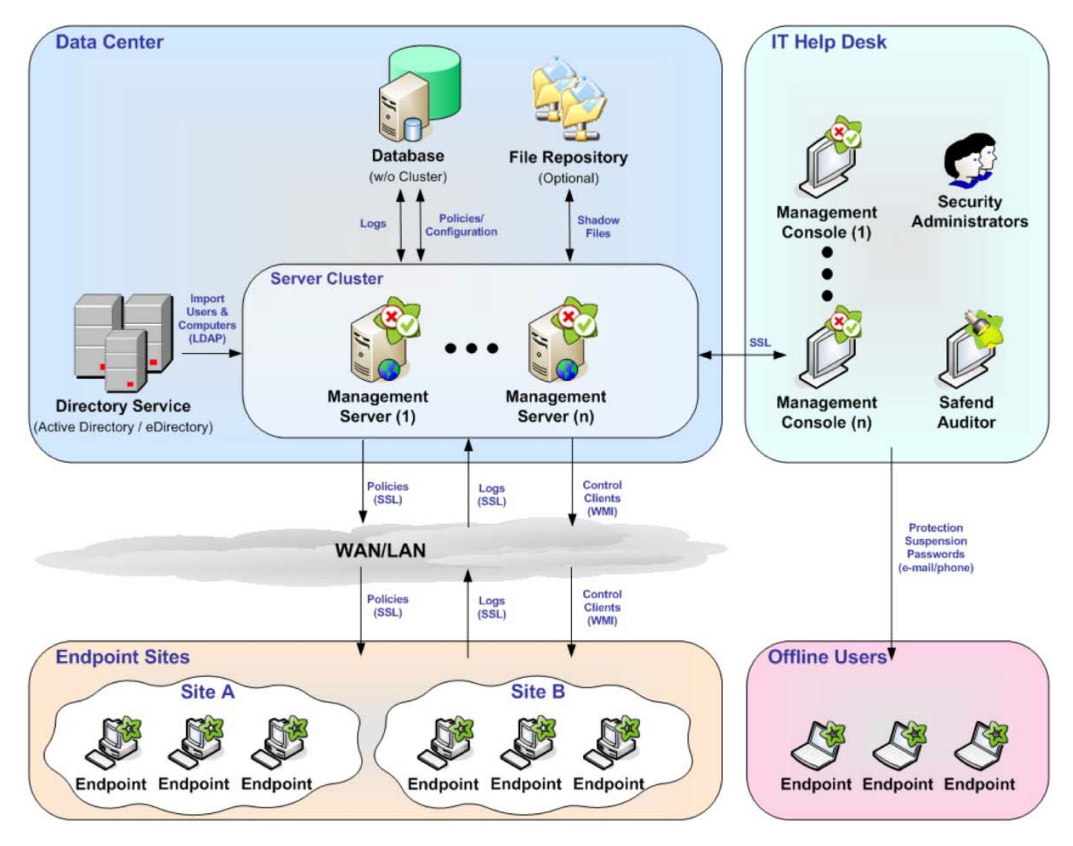



Weitere Informationen finden Sie im *SafeGuard PortAuditor Benutzerhandbuch*.

## 1.3 Systemarchitektur



Die folgende Abbildung zeigt die Systemarchitektur:




Das System besteht aus folgenden Komponenten:

- **SafeGuard PortProtector Management Server –** SafeGuard PortProtector Management Server speichern die Policies und andere Definitionen, erfassen Logs von den Clients, ermöglichen das Client-Management und verteilen Policies an die Clients. Als Speicher nutzen die Management Server eine interne bzw. externe Datenbank (siehe unten).

  Für die Kommunikation mit den Clients und der Management Console setzen die Management Server IIS ein (über SSL). Die Kontrolle der Clients erfolgt über WMI. LDAP-konforme Protokolle werden zur Synchronisierung mit vorhandenen Organisationsobjekten genutzt, die in einem Active Directory/Novell eDirectory gespeichert sind. Normalerweise verteilen die Management Server die Policies direkt an die Clients (über SSL). Außerdem wird eine alternative Verteilungsmethode unterstützt, die den Active Directory GPO-Mechanismus nutzt. GPOs mit Policies werden in das Active Directory geschrieben. Nachdem die Policies mit den Einheiten der Organisation verknüpft wurden, werden sie auf die Endpunkte heruntergeladen und dort angewendet.

- **Interne/externe Datenbank** – Zur Speicherung der Systemkonfiguration, Policies und Logdaten werden Standarddatenbanken eingesetzt. Die Administratoren können entweder eine interne MySQL-Datenbank verwenden, die mit dem Management Server-Installationspaket geliefert wird, oder eine Verbindung zu vorhandenen MSSQL-Datenbankinfrastrukturen herstellen. Der Einsatz der internen Datenbank ist einfacher und wartungsfrei. Die Verbindung zu einer externen Datenbank bietet hingegen bessere Performance und Skalierbarkeit. Beachten Sie, dass ein Serverzusammenschluss nur mit einer externen MSSQL-Datenbank möglich ist.
- **SafeGuard PortProtector Management Console –** ermöglicht es Ihnen, Client zu verwalten, Logs anzuzeigen, Policies zu definieren und das System zu verwalten. Die Management Console kann auf jedem beliebigen Computer in Ihrem Netz installiert und ausgeführt werden. Zur Kommunikation mit dem Management Server wird SSL eingesetzt. Die Management Console ermöglicht das Deployment über die Server-Website per Mausklick.
- **SafeGuard PortProtector Client –** schützt und überwacht die Endpunkte in Ihrer Organisation und alarmiert/informiert über die Portaktivitäten. Der Client kommuniziert mittels SSL mit einem SafeGuard PortProtector Management Server.
- **SafeGuard PortAuditor –** Auch wenn SafeGuard PortAuditor kein integraler Bestandteil von SafeGuard PortProtector ist, geht dieses clientlose Tool doch mit SafeGuard PortProtector Hand in Hand und ergänzt das System mit einer kompletten Sicht darauf, welche Ports, Geräte und Netze von den Benutzern in Ihrer Organisation genutzt werden (oder früher genutzt wurden. Mit Hilfe eines SafeGuard PortAuditor-Scans können Sie die Geräte und Netze auswählen, deren Nutzung Sie genehmigen möchten.
- **SafeGuard PortProtector Management Server Cluster –** Durch ein Server-Cluster ist die Installation mehrerer SafeGuard PortProtector Management Servers möglich, die an eine einzige externe Datenbank angeschlossen werden, so dass sie die Verkehrslast von den Endpunkten problemlos teilen und Redundanz sowie hohe Verfügbarkeit bieten können.

  Ein solcher Serverzusammenschluss kann nur bei Systemen mit einer externen MSSQL-Datenbank (nicht mit einer internen Datenbank), auf die von allen Servern des Clusters zugegriffen werden kann, erstellt werden. Diese Server teilen sich eine einzelne MSSQL-Datenbank oder ein MSSQL-Datenbankcluster.

  Die Liste der verfügbaren Server wird routinemäßig an die Clients übertragen. Diese wählen im Zufallsprinzip den Server, mit dem sie sich verbinden möchten, um eine gleichmäßige Verteilung der Last auf die Server sicherzustellen. Falls die Verbindung zu einem bestimmten Server fehlschlägt, wählt der Client sofort einen anderen Server und stellt die Verbindung zu ihm her.

**Hinweis:** Management Consoles stellen die Verbindung zu dem Server her, von dem aus sie ursprünglich installiert wurden.

## 1.4 SafeGuard PortProtector Management Console

Die SafeGuard PortProtector Management Console ist ein vereinheitlichtes Managementtool, mit dem Ihre IT- bzw. Sicherheitsabteilung Berechtigungen über Policies definieren, Clients verwalten und Port-, Geräte- und Netzwerknutzung in Ihrer Organisation überwachen kann.

### 1.4.1 So funktioniert es

Die Management Console wird mit Ihrem Active Directory oder Novell eDirectory integriert, so dass Sie Policies einfach mit den Computern und Benutzern in Ihrem Netz verknüpfen können. Die Verteilung der Policies erfolgt normalerweise direkt von den Servern an die Endpunkte (über SSL). Weitere Möglichkeiten sind die bewährten Mechanismen für die Gruppenpolicy oder Tools von Drittanbietern, die Sie evtl. in Ihrem Netz einsetzen.

Die SafeGuard PortProtector Management Console wird während der Serverinstallation automatisch auf demselben Computer wie der SafeGuard PortProtector Management Server installiert. Bei Bedarf kann sie auf weiteren Computern installiert werden.

Anschließend können Sie Policies definieren, wie in *Kapitel 3*, *Definieren von* Policies, *beschrieben.*

Im Anschluss an die Verteilung der Policies und deren Anwendung auf den Endpunkten können Sie die Logeinträge in der Logs-Welt anzeigen, wie in *Kapitel 5, Anzeigen von* Logs, beschrieben.

### 1.4.2 Definition der Policy

#### 1.4.2.1 Was wird durch eine Policy definiert?

Jede Policy definiert zwei Arten von Informationen – **Sicherheit**sdefinitionen und Policy-**Einstellungen** – wie folgt:

- **Sicherheit**sdefinitionen spezifizieren die Policy (gesperrt, zugelassen oder eingeschränkt) für den Zugriff auf die Ports an den Endpunkten in Ihrer Organisation:
- Die **Portkontrolle** spezifiziert die Policy Ihrer Organisation im Hinblick auf den Portzugriff an den Endpunkten.
- Die **Gerätekontrolle** spezifiziert die Policy Ihrer Organisation hinsichtlich der Geräte, die berechtigt sind auf USB-, PCMCIA- und FireWire-Ports an den Endpunkten zuzugreifen.
- Die **Speicherkontrolle** spezifiziert die Policy Ihrer Organisation hinsichtlich der Speichergeräte, die berechtig sind auf USB-, PCMCIA- und FireWire-Ports an den Endpunkten zuzugreifen (einschließlich Verschlüsselung von Wechselspeichergeräten). In diesem Schritt definieren Sie auch, ob die Daten auf Ihren internen Festplatten verschlüsselt werden oder nicht.
- Die **Dateikontrolle** spezifiziert die Policy Ihrer Organisation hinsichtlich der Dateien, die zu/von externen Speichergeräten übertragen werden. Dadurch werden die Übertragungen nach Dateityp und tatsächlichem Inhalt kontrolliert.
- Die **WiFi-Kontrolle** spezifiziert die Policy Ihrer Organisation hinsichtlich der WiFi-Links, auf die die Endpunkte zugreifen dürfen.

- Die **Einstellungen** spezifizieren, wie sich die Policy auf den Endpunkten verhält:
- Die **Protokollierung** spezifiziert die Protokollierungseinstellungen für die Policy, wie etwa die Häufigkeit mit der Logeinträge von einem geschützten Endpunkt aus an einen SafeGuard PortProtector Management Server gesendet werden.
- **Alarme** gibt die Ziele an, an die Alarme für die Policy gesendet werden sollen.
- Mit **Endbenutzer-Meldungen** können Sie die Standardmeldungen bearbeiten, die auf einem geschützten Endpunkt während der laufenden Benutzung und beim Auftreten einer Policy-Verletzung angezeigt werden.
- **Die Mediaverschlüsselung** bestimmt das Verhalten des Systems, wenn die Berechtigungen eines Wechselspeichergeräts eine Verschlüsselung erforderlich machen.
- Die **Inhaltsprüfung** (nur verfügbar, wenn Inhaltsprüfung aktiviert ist) definiert die für die Inhaltsprüfung erforderlichen Einstellungen, wie beispielsweise Einstellungen für die Alarmversendung, Größe des Datei-Caches etc.
- Über die **Optionen** können Sie die verschiedenen Verhaltensaspekte der Policy zu definieren, z. B. die Art und Weise, in der aktive Geräte bei Bedarf getrennt werden.

Dies alles ist detailliert in *Kapitel 3, Definieren von* Policies*, beschrieben.*

### 1.4.2.2 Wie wird eine Policy definiert?

SafeGuard PortProtector-Policies werden in der SafeGuard PortProtector Management Console definiert. Sie können entweder eine Policy für Ihre gesamte Organisation oder angepasste Policies für jede in Ihrem Active Directory oder Novell eDirectory definierte Organisationseinheit (Computer bzw. Benutzer) festlegen.

Die Policies müssen einmal definiert werden. Danach werden Sie bei Bedarf aktualisiert. Um eine neue Policy zu definieren, legen Sie einfach alle oben genannten Aspekte der Policy fest und speichern sie.

*Kapitel 4, Verteilen von* Policies, beschreibt die Optionen für das Verteilen von Policies direkt von den Servern, über Microsoft Active Directory GPO oder über Registry-Dateien.

Sobald Sie eine Policy definiert und an die SafeGuard PortProtector Clients verteilt haben, können Sie die Aktivitätenlogs von jedem Client über die Logs-Welt in der SafeGuard PortProtector Management Console anzeigen, wie in *Kapitel 5, Anzeigen von* Logs, beschrieben. Die Logeinträge enthalten zahlreiche Informationen, wie etwa:

- Policy-Verletzungen, wie etwa der Versuch, ein gesperrtes Gerät zu benutzen
- die Nutzung von schreibgeschützten Speichergeräten
- die Verteilung neuer Policies

Nach der Analyse der Logs können Sie Ihre Policies ggf. anpassen. Eine detaillierte Informationen darüber, wie Policies definiert werden, finden Sie in *Kapitel 3, Definieren von* Policies.

## 1.5 Durchsetzung der SafeGuard-Policy – SafeGuard PortProtector Client

Der SafeGuard PortProtector Client ***überwacht*** ständig den Echtzeitverkehr auf den geschützten Ports und wendet angepasste, ausgefeilte Sicherheitspolicies auf alle physischen, kabellosen und Wechselspeicher-Schnittstellen an. Er ***sperrt*** unberechtigte Aktivitäten (wie etwa Gerät einstecken, auf das Speichergerät schreiben, an WiFi-Netze anschließen), ***schützt*** die auf die Speichergeräte geschriebenen Daten, ***alarmiert*** die Administratoren über unberechtigte Nutzungsversuche und ***protokolliert*** Ereignisse für künftige Ansicht und Auswertung.

Der SafeGuard PortProtector Client ist ein Softwarepaket, das transparent auf den Endpunkt-Computern auf Kernelebene läuft und die Schutzpolicies auf jedem Rechner, auf dem es eingesetzt ist, durchsetzt. Die Software benötigt nur minimalen Platz (in puncto Dateigröße, CPU- und Speicherressourcen) und beinhaltet redundante Multi-Tier-Funktionen zum Schutz vor Manipulationen, um eine permanente Kontrolle der Endpunkte zu gewährleisten.

SafeGuard PortProtector Client kann unbemerkt auf allen Endpunkten installiert werden.

Die Verteilung der Policy an die Endpunkt-Computer kann entweder durch den Management Server über SLL oder mit Hilfe der Group Policy Management Console des Microsoft Active Directory oder mit Hilfe eines beliebigen, in Ihrer Organisation zur Verteilung von Software eingesetzten Tools eines Drittanbieters erfolgen.

Sobald die Policies verteilt wurden beginnt der Client sofort mit dem Schutz der Ports des Computers. Ein Neustart ist hierfür nicht erforderlich.

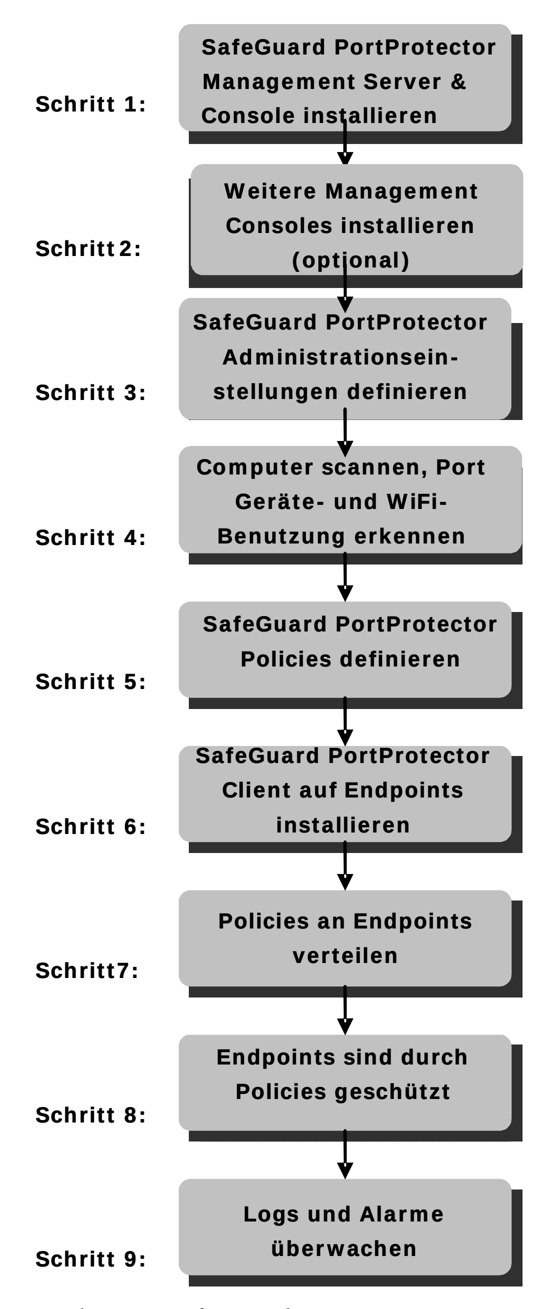
Bei einer Verletzung einer SafeGuard PortProtector-Policy oder bei bestimmten Nutzungsaktivitäten wird eine Meldung auf dem Computer des Endpunkts angezeigt. Eine Policy-Verletzung bedeutet, dass jemand versucht hat, einen Port, ein Gerät oder einen WiFi-Link zu benutzen, die auf einem mit SafeGuard PortProtector geschützten Computer gesperrt wurden. Der Endbenutzer kann einfach auf die Meldung klicken und so bestätigen, dass er sie gelesen hat. Je nach den in Ihrer Policy definierten Einstellungen kann ein Logeintrag erzeugt werden, der dieses Ereignis aufzeichnet.

Sie können den Client im Stealth-Modus installieren und sowohl das SafeGuard PortProtector Taskleistensymbol als auch Meldungen ausblenden. Auf diese Weise machen Sie den SafeGuard PortProtector Client für den Benutzer am Endpunkt unsichtbar.

Weitere Informationen finden Sie im *Kapitel Endbenutzer-Erfahrung*.

## 1.6 Workflow zur Implementierung von SafeGuard PortProtector

Im Folgenden finden Sie eine Übersicht über den Workflow für die Implementierung und Nutzung von SafeGuard PortProtector.




- **Schritt 1: SafeGuard PortProtector Management Server und Console installieren:** wie im *SafeGuard PortProtector Installationshandbuch* beschrieben.
- **Schritt 2: Weitere Management Consoles installieren:** wie im *SafeGuard PortProtector Installationshandbuch* beschrieben.
- **Schritt 3: Allgemeine SafeGuard PortProtector Administrationseinstellungen definieren,** z. B. auf welche Weise Policies veröffentlicht werden: wie in *Kapitel 8, Administration*, beschrieben.

- **Schritt 4: Computer scannen und Port-/Gerätenutzung erkennen:** Verwenden Sie SafeGuard PortAuditor, um die Ports zu erkennen, die in Ihrer Organisation genutzt wurden, sowie die Geräte und WiFi-Netze, die an diesen Ports angeschlossen waren, wie im *SafeGuard PortAuditor Benutzerhandbuch* beschrieben.
- **Schritt 5: SafeGuard PortProtector-Policies definieren:** In diesem Schritt definieren Sie die gesperrten, zugelassen und eingeschränkten Ports, Geräte und WiFi-Netze gemäß den Sicherheits- und Produktivitätsanforderungen Ihrer Organisation, wie in *Kapitel 3, Definieren von Policies*, beschrieben.
- **Schritt 6: SafeGuard PortProtector Client auf Endpunkten installieren:** wie im *SafeGuard PortProtector Installationshandbuch* beschrieben.
- **Schritt 7: SafeGuard PortProtector-Policies an Endpunkte verteilen:** In diesem Schritt können Sie Policies zu Benutzern und Computern zuordnen und sie direkt (via SSL) an die Endpunkte verteilen, oder die GPO-Funktion von Active Directory oder ein beliebiges Tool eines Drittanbieters zur Verteilung von SafeGuard PortProtector-Policies nutzen, wie in *Kapitel 4, Verteilen von* Policies, beschrieben.
- **Schritt 8: Endpunkte sind durch SafeGuard PortProtector-Policies geschützt**: In diesem Schritt können nur zugelassene Geräte und WiFi-Netze auf freigegebenen Ports genutzt werden. Logs über Port-, Geräte- und WiFi-Netzwerknutzung und Nutzungsversuche sowie Manipulationsversuche werden erstellt und an den Management Server gesendet, wie in *Kapitel 9, Endbenutzer-Erfahrung*, beschrieben.
- **Schritt 9: Logs und Alarme überwachen:** Anzeige und Export der von den SafeGuard PortProtector Clients generierten Logeinträge, wie in *Kapitel 5, Anzeigen von* Logs, *beschrieben.*

# 2 Erste Schritte

## Über dieses Kapitel

Dieses Kapitel beschreibt zunächst, wie die SafeGuard PortProtector Management Console gestartet wird. Danach folgt ein kurzer Überblick über die Benutzeroberfläche der SafeGuard PortProtector Management Console, bei dem die Hauptfenster und Menüs und das *Home*-Registerfenster, oder auch die 'Home-Welt', beschrieben werden. Es enthält die folgenden Abschnitte:

- ***Starten der SafeGuard PortProtector Management Console*** beschreibt, wie die Management Console gestartet wird.
- ***Übersicht über die Anwendung*** beschreibt die Hauptabschnitte und Schaltflächen in der Anwendung.
- ***Welten*** beschreibt die wesentlichen Registerkarten, die sich jeweils mit einem anderen Aspekt der Anwendung befassen.
- ***Menüleiste*** beschreibt die Menüoptionen in der SafeGuard PortProtector Management Console.
- ***Fensterleiste und Fensteroptionen*** beschreibt diese spezielle Leiste, die in einigen der Anwendungsfenster vorhanden ist, sowie deren Steuerungen. Auch die in einigen Fenstern verfügbaren Funktionen werden beschrieben, wie etwa das Duplizieren und Lösen eines Fensters.
- ***Start-Welt*** beschreibt das das Einstiegsfenster der SafeGuard PortProtector Management Console.

## 2.1 Starten der SafeGuard PortProtector Management Console

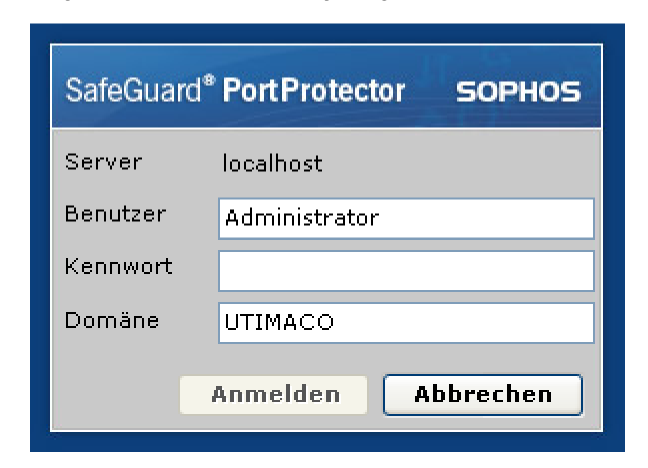
Starten Sie die SafeGuard PortProtector Management Console wie folgt.

**So melden Sie sich an:**

Klicken Sie auf Ihrem Desktop auf das Symbol ,

ODER

Wählen Sie Start → Programme → SafeGuard PortProtector → Management Console. Das folgende Fenster wird angezeigt:




1 Geben Sie Ihren Benutzernamen, Ihr Kennwort und die Domäne ein.

2 Klicken Sie auf **Anmelden**.

3 Wenn Sie eine permanente Lizenz erworben und das voreingestellte globale Kennwort für die Deinstallation von SafeGuard PortProtector Clients noch nicht geändert haben, werden Sie dazu im nachfolgend angezeigten Fenster aufgefordert:

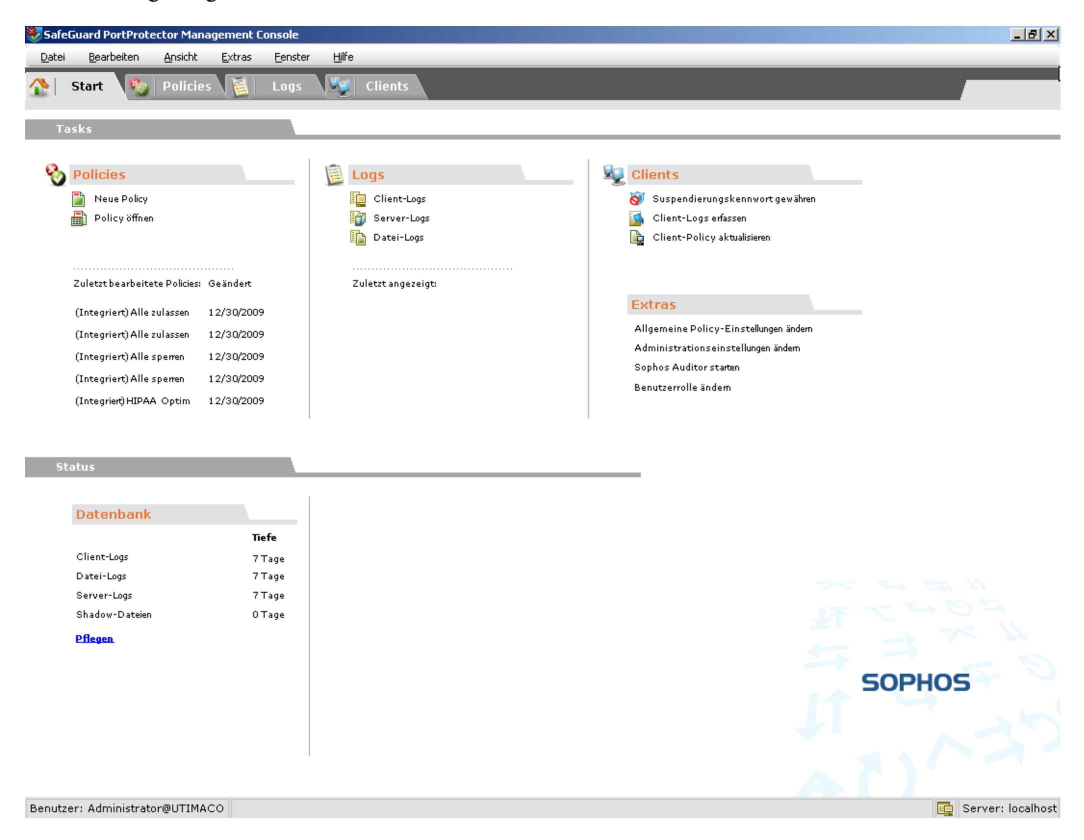



4 Klicken Sie auf **OK**. Die Anwendung wird geöffnet und das Hauptfenster wird angezeigt.

**Hinweis:** Einem SafeGuard PortProtector-Administrator können mehrere Rollen zugewiesen werden, um die verschiedenen Domänenpartitionen zu definieren, für die er verantwortlich ist. Nachdem sich ein solcher Administrator angemeldet hat, wird automatisch ein Auswahlfenster angezeigt, in dem er die entsprechende Rolle für seine Arbeit auswählen kann. Eine Benutzerrolle definiert die Funktionen, Organisationseinheiten und Domänen einer Organisation, auf die ein SafeGuard PortProtector-Administrator zugreifen kann (siehe auch Definieren von Rollen).

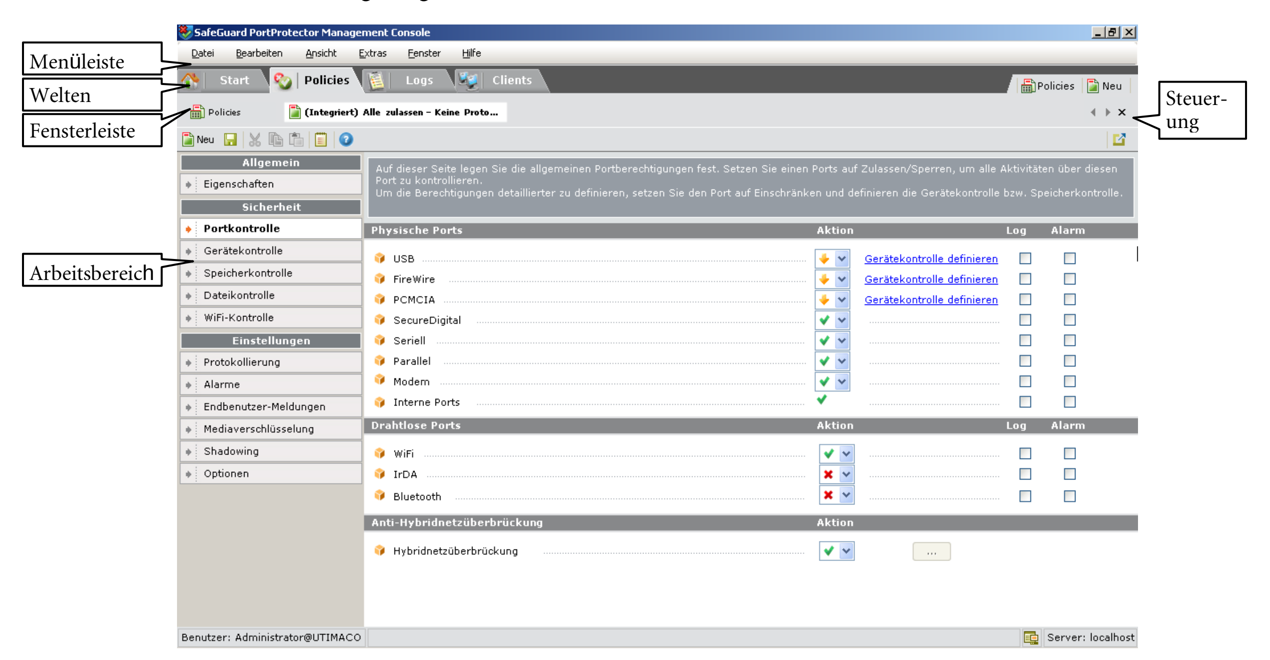
## 2.2 Übersicht über die Anwendung

Nach der Anmeldung bei der SafeGuard PortProtector Management Console wird das folgende Fenster angezeigt:




Dies ist die Start-Registerkarte. Sie zeigt die Home-Welt, die in *Start-Welt* erläutert wird.

Da dies kein typisches Fenster ist, wechseln Sie bitte zur Registerkarte Policies. Das folgende Fenster wird angezeigt:




Das Fenster enthält folgende Bereiche:

- **Welten-Registerkarten** – jede Registerkarte, oder Welt, beinhaltet einen anderen Aspekt der Anwendung (siehe *Welten*).
- **Menüleiste** – zeigt die Menüs.
- **Fensterleiste** – zeigt die Namen der geöffneten Fenster in der Policies- und in der Logs-Welt.
- **Symbolleiste** – hier finden Sie verschiedene Funktionen, die für die Registerkarten Policies, Logs und Clients unterschiedlich sind.
- **Steuerungsschaltflächen** – vereinfachen das Öffnen und die Handhabung der Fenster in der Policies-**Welt** und Logs-Welt.
- **Arbeitsbereich** – bietet je nach aktiver Welt andere Informationen und Optionen, die in späteren Kapiteln beschrieben werden. Die Home-Welt, die als Erste nach dem **Start** der SafeGuard PortProtector Management Console angezeigt wird, ist in *Start-Welt* beschrieben.

## 2.3 Welten

Die SafeGuard PortProtector Management Console besteht aus vier Registerkarten. Jede Registerkarte, oder **Welt**, verwaltet einen anderen Aspekt der Anwendung:

- **Start** – diese Welt, die in *Start-Welt* beschrieben ist, liefert sowohl eine Übersicht über die gängigsten Aufgaben als auch Informationen aus anderen Welten. Sie ist die zentrale Stelle, von der aus Sie diese Aufgaben aktivieren und auf die Informationen zugreifen können.
- **Policies** – in dieser Welt, die im Kapitel *Definieren von Policies*, beschrieben ist, **definieren** und verwalten Sie die Policies, einschließlich Port-, Geräte- und WiFi-Berechtigungen, freigegebener Geräte und Netze (White List), Verschlüsselung der Wechselspeichergerät etc.
- **Logs** – in dieser Welt, die im Kapitel *Anzeigen von Logs*, beschrieben ist, können Sie die **Logs**, die von geschützten Clients gesendet wurden, abfragen, anzeigen und verwalten.
- **Client** – in dieser Welt, die im Kapitel *Verwalten von Clients*, beschrieben ist, zeigen Sie Client-Eigenschaften und -Status an, aktualisieren Client-Policies, erzeugen ein Client-Suspendierungskennwort etc.

## 2.4 Menüleiste

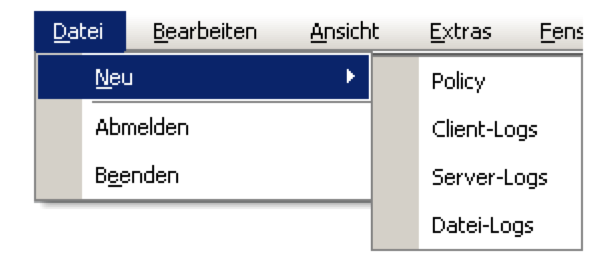
Einige Menüs in der SafeGuard PortProtector Management Console sind in allen Welten vorhanden (die Menüs *Bearbeiten, Extras* und *Fenster*), wohingegen andere unterschiedlich sind. Die gemeinsamen Menüs sowie das für die Home-Welt spezifische Menü werden hier beschrieben.

Die Menüleiste enthält die folgenden Optionen:




### 2.4.1 Menü Datei

Über das Menü *Datei* in der Start-Welt können Sie neue Policy-Fenster und Log-Fenster öffnen, sich von der Management Console abmelden und die Anwendung beenden.

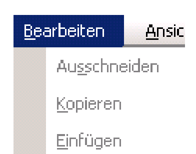


Das Menü *Datei* enthält folgende Optionen:

| Option | Beschreibung |
| --- | --- |
| **Neu** | Öffnet ein Untermenü, über das Sie ein neues Policy-Fenster, ein neues Client Log-Fenster, ein neues Server Log-Fenster oder ein neues File Log-Fenster öffnen können. |
| **Benutzerrolle ändern** | Einem SafeGuard PortProtector-Administrator können mehrere Rollen zugewiesen werden, um die verschiedenen Domänenpartitionen zu definieren, für die er verantwortlich ist. Nachdem sich ein solcher Administrator angemeldet hat, wird automatisch ein Auswahlfenster angezeigt, in dem er die entsprechende Rolle für seine Arbeit auswählen kann.<br>**Hinweis:** Eine Benutzerrolle definiert die Funktionen, Organisationseinheiten und Domänen einer Organisation, auf die ein SafeGuard PortProtector-Administrator zugreifen kann, wie in *Definieren von Rollen* beschrieben.<br>Über die Option **Benutzerrolle ändern** kann ein solcher Administrator von dieser Rolle jederzeit zu einer anderen, ihm zugewiesenen Rolle wechseln. |
| **Abmelden** | Meldet den aktuellen Benutzer von der Management Console ab. |
| **Beenden** | Meldet den aktuellen Benutzer ab und schließt die SafeGuard PortProtector Management Console. |

## 2.4.2 Menü Bearbeiten

Das Menü *Bearbeiten* ist in allen Welten vorhanden, auch wenn die Menüoptionen in allen außer der Policies-Welt deaktiviert sind. Es umfasst die Optionen **Ausschneiden**, **Kopieren** und **Einfügen** für die Option **Gerät hinzufügen, Speichergerät hinzufügen** oder **WiFi-Netz hinzufügen** dies ist in Freigeben von Geräten und WiFi-Verbindungen im Kapitel *Definieren von Policies* beschrieben.



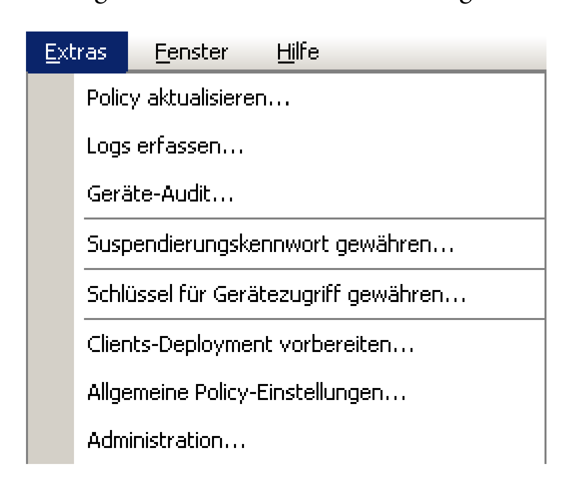
## 2.4.3 Menü Ansicht

Über das Menü *Ansicht* in der Start-Welt können Sie den Verlauf der Client-Tasks anzeigen. Weitere Informationen zu Client-Tasks finden Sie in Verfolgen des Fortschritts von Client-Tasks im *Verwalten von Clients*.




## 2.4.4 Menü Extras

Das Menü *Extras* haben alle Welten gemeinsam. Über dieses Menü können Sie verschiedene Management- und Administratoraufgaben ausführen.




Das Menü *Extras* enthält folgende Optionen:

| Option | Beschreibung |
|---|---|
| **Policy aktualisieren** | Aktualisiert Policies (weitere Informationen hierzu finden Sie im Kapitel *Verwalten von Clients*). |
| **Logs erfassen** | Erfasst Logs (weitere Informationen hierzu finden sie in *Abrufen der aktuellsten Informationen von einem* Client im Kapitel *Verwalten von Clients).*<br><br>**Anmerkung:** Auf diese Option können Sie auch zugreifen, indem Sie in der Clients-Welt mit der rechten Maustaste auf diesen Client klicken. |
| **Geräte-Audit** | Startet SafeGuard PortAuditor. |

| Option | Beschreibung |
|---|---|
| **Suspendierungs-kennwort gewähren** | Erstellt einen Schlüssel, der dazu genutzt werden kann, einen Suspendierungsschlüssel zu gewähren, damit ein Benutzer den Schutz temporär aufheben kann (weitere Informationen zu *Vorübergehende Aufhebung des* SafeGuard-Schutzes finden Sie in *Kapitel 6, Verwalten von Clients).*<br><br>**Hinweis:** Auf diese Option können Sie auch zugreifen, indem Sie in der Clients-Welt mit der rechten Maustaste auf diesen Client klicken. |
| **Clients-Deployment vorbereiten** | Erläutert, was für das Deployment von Clients und Ports für die Position der Installationsdateien erforderlich ist. |
| **Allgemeine Policyein-stellungen** | Ermöglicht die Anzeige und Änderung der globalen Policy-Einstellungen (weitere Informationen hierzu finden Sie in *Schritt 9: Allgemeine Policy-Einstellungen definieren* im Kapitel *Definieren von Policies*).<br><br>**Anmerkung:** Auf diese Option können Sie auch zugreifen, indem Sie in der Clients-Welt mit der rechten Maustaste auf diesen Client klicken. |
| **Administration** | Ermöglicht es dem Administrator, administrative Aufgaben auszuführen (weitere Informationen hierzu finden Sie in *Fenster Administration* im Kapitel *Administration*). |

### 2.4.5 Menü Fenster

Das Menü *Fenster* haben alle Welten gemeinsam. Über dieses Menü können Sie zu anderen Welten wechseln, weitere Fenster öffnen und Fenster in der Policies-Welt und Logs-Welt duplizieren, lösen und schließen (diese Optionen werden in *Fensterleiste und Fensteroptionen* erklärt).



Das Menü *Fenster* enthält folgende Optionen:

| Option | Beschreibung |
|---|---|
| **Duplizieren** | Diese Option ist nur in der Policies-Welt und in der Logs-Welt verfügbar. |
| **Lösen** | Diese Option ist nur in der Policies-Welt und in der Logs-Welt verfügbar. |
| **Schließen** | Diese Option ist nur in der Policies-Welt und in der Logs-Welt verfügbar. |
| **Start** | Öffnet die Start-Welt. |
| **Policies** | Öffnet die Policies-Welt. |
| **Logs** | Öffnet die Logs-Welt. |
| **Clients** | Öffnet die Clients-Welt. |

### 2.4.6 Menü Hilfe

Das Menü *Hilfe* liefert Informationen zu SafeGuard PortProtector.



Das Menü *Hilfe* haben alle Welten gemeinsam, und es enthält folgende Optionen:

| Option | Beschreibung |
|---|---|
| **Hilfethemen** | Öffnet die SafeGuard PortProtector Policy Builder-Hilfe. |
| **Info** | Zeigt Urheberrecht- und Lizenzinformationen zu SafeGuard PortProtector sowie Kontaktinformationen für Sophos an. |




## 2.5 Fensterleiste und Fensteroptionen

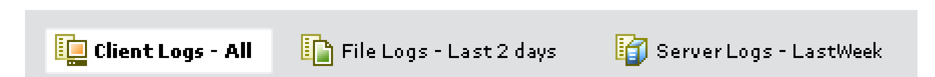
In der Policies-Welt und in der Logs-Welt können mehrere Fenster geöffnet werden. Die Fensterleiste zeigt geöffnete Fenster.

### 2.5.1 Fensterleiste

In der Policies-Welt können Sie zusätzlich zum Hauptfenster, in dem Sie Policies verwalten, mehrere Policies jeweils in einem eigenen Fenster öffnen. Die Fensterleiste zeigt die Namen der geöffneten Policies an:




In der Logs-Welt können Sie mehrere Logs jeweils in einem eigenen Fenster öffnen. Die Fensterleiste zeigt die Namen der geöffneten Logabfragen an:



## 2.5.2 Steuerungsschaltflächen

Zum Öffnen, Verwalten und Navigieren der Fenster in der Policies-Welt und in der Logs-Welt stehen mehrere Steuerungsschaltflächen zur Verfügung. Diese Schaltflächen erscheinen oben rechts in jedem Fenster.

- **Startschaltflächen** Client-Logs Datei-Logs Server-Logs, oben rechts in Policies- oder Logs-Fenstern – mit Hilfe dieser Schaltflächen können Sie weitere Fenster öffnen. Die Startschaltflächen sind in der Policies-Welt und in der Logs-Welt unterschiedlich. Sie werden in den jeweiligen Kapiteln erläutert.
- **Navigationsschaltflächen** – mit den Pfeilen nach links und nach rechts können Sie weitere geöffnete Fenster anzeigen, wenn mehr Fenster geöffnet sind als in der **Fensterleiste** angezeigt werden können.
- **Close-Schaltfläche** × – neben den Navigationsschaltflächen – hiermit schließen Sie das aktive Fenster (das **aktive** Fenster ist das derzeit angezeigte Fenster, dessen Name in der Fensterleiste hervorgehoben ist).
- **Lösen-Schaltfläche** – hiermit lösen Sie das aktive Fenster (das aktive Fenster ist das derzeit angezeigte Fenster, dessen Name in der Fensterleiste hervorgehoben ist). Eine Erklärung zum Lösen von Fenstern finden Sie in *Fenster lösen und andocken*.
- **Andocken-Schaltfläche** – wenn ein Fenster gelöst wurde, erscheint statt der **Lösen-Schaltfläche** die **Andocken**-Schaltfläche. Klicken Sie darauf, um das Fenster wieder in seiner Welt anzudocken. Eine Erklärung zum Lösen von Fenstern finden Sie in *Fenster lösen und andocken*.

### 2.5.3 Optionen für aktives Fenster

Das aktive Fenster ist das derzeit angezeigte Fenster, dessen Name in der Fensterleiste hervorgehoben ist. Das aktive Policy-Fenster in der Policies-Welt und das aktive Log-Fenster in der Logs-Welt kann dupliziert, gelöst und geschlossen werden.

#### 2.5.3.1 Fenster duplizieren

Eventuell möchten Sie ein Fenster z. B. in der Policies-Welt duplizieren, um eine Policy als Ausgangspunkt für eine andere zu nutzen, oder in der Logs-Welt, um dieselbe Abfrage für verschiedene Elemente in der Organisationsstruktur auszuführen.

**So duplizieren Sie das ausgewählte Fenster:**

Klicken Sie im Menü *Fenster* auf **Duplizieren**.

ODER

1. Klicken Sie in der Fensterleiste mit der rechten Maustaste auf den Namen des zu duplizierenden Fensters. Das ausgewählte Fenster wird aktiv, und es wird ein Menü angezeigt.
2. Klicken Sie im Menü auf **Fenster duplizieren**.

Es wird ein neues Log-Fenster geöffnet, das mit dem angezeigten Fenster identisch ist.

#### 2.5.3.2 Fenster lösen und andocken

Beim Lösen eines Fensters wird es von seiner Welt-Registerkarte getrennt und unabhängig. Das ist vor allem dann hilfreich, wenn Sie in eine andere Welt wechseln und das aktive Fenster weiter geöffnet halten möchten.

**So lösen Sie das aktive Fenster:**

Klicken Sie im Menü *Fenster* auf **Lösen**.

ODER

Klicken Sie oben rechts im aktiven Fenster auf die **Lösen**-Schaltfläche.

ODER

1. Klicken Sie in der Fensterleiste mit der rechten Maustaste auf den Namen des zu lösenden Fensters. Das ausgewählte Fenster wird aktiv, und es wird ein Menü angezeigt.
2. Klicken Sie im Menü auf **Fenster lösen**.

Das aktive Fenster ist jetzt separat und unabhängig.

Sie können ein gelöstes Fenster bei Bedarf wieder andocken.

**So docken Sie ein gelöstes Fenster an:**

Klicken Sie oben rechts im aktiven Fenster auf die **Andocken**-Schaltfläche. Das Fenster wird wieder in seiner Welt angedockt.

#### 2.5.3.3 Fenster schließen

**So schließen Sie das aktive Fenster:**

Klicken Sie auf die **Schließen**-Schaltfläche ×, die sich in der oberen rechten Ecke des Fensters befindet.

ODER

1 Klicken Sie in der Fensterleiste mit der rechten Maustaste auf den Namen des zu schließenden Fensters. Das ausgewählte Fenster wird aktiv, und es wird ein Menü angezeigt.

2 Klicken Sie im Menü auf **Fenster schließen**.

Das Fenster wird geschlossen.

#### 2.5.3.4 Zwischen geöffneten Fenstern navigieren

In manchen Situationen sind mehr Fenster geöffnet als in der *Fensterleiste* angezeigt werden können. Sie können dann nach rechts oder links zum gewünschten Fenster navigieren.

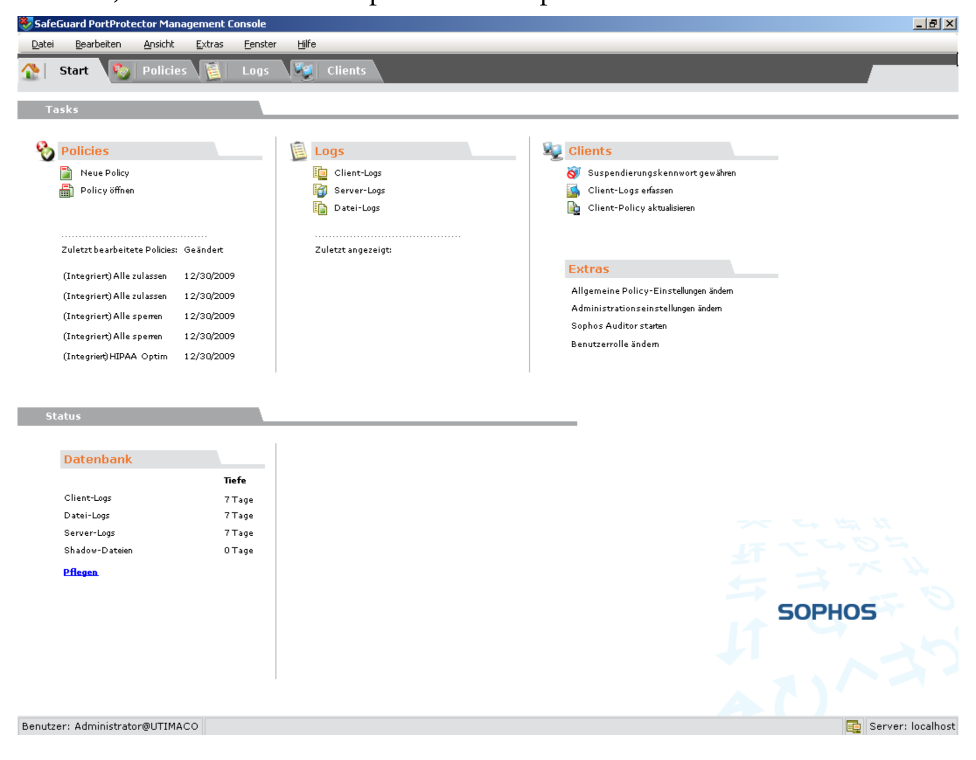
**So navigieren Sie zwischen geöffneten Fenstern:**

Klicken Sie auf die Rechts- oder Links-Pfeile ◀ ▶ in der oberen rechten Ecke des Fensters, bis das gewünschte Fenster in der Fensterleiste sichtbar ist.

## 2.6 Start-Welt

Die Start-Welt stellt den zentralen Zugangspunkt zu den gängigsten Aufgaben und aktuellen Informationen aus den anderen Welten dar.

**Hinweis:** Hier wird eine allgemeine Beschreibung der über die Start-Welt zugänglichen Aufgaben und Informationsarten gegeben. Um mehr über die einzelnen Aufgaben/Informationsarten zu erfahren, lesen Sie bitte die entsprechenden Kapitel in diesem Benutzerhandbuch.



## 2.6.1 Start-Welt – Beschreibung

Der Arbeitsbereich ist in zwei Bereiche unterteilt: Tasks und Status.

### *Tasks*

Dieser Bereich in der oberen Hälfte des Fensters enthält Links und Tool-Schaltflächen für den Zugriff auf die Informationen und die wesentlichsten Funktionen aus anderen Welten. Alle diese Funktionen können von jeder Welt aus über die Menüs, Schaltflächen der Symbolleiste bzw. Kontextmenüs ausgeführt werden. Der Bereich ist in vier Abschnitte unterteilt, wie nachfolgend beschrieben:

- **Policies:** Durch Klicken auf den Titel des Abschnitts wird in die Policies-Welt gewechselt. Dieser Abschnitt enthält Symbole und Links zu Folgendem:
  - **Neue Policy –** klicken Sie hierauf, um eine neue Policy zu definieren.
  - **Policy öffnen –** klicken Sie hierauf, um eine vorhandene Policy zu öffnen. Das Fenster Policy Management wird angezeigt.
  - **Zuletzt bearbeitete Policies –** hier wird eine Liste der letzten fünf bearbeiteten Policies zusammen mit dem Änderungsdatum angezeigt. Zum Öffnen klicken Sie auf die gewünschte Policy.

Eine detaillierte Erläuterung zu Definition und Management von Policies finden Sie in Kapitel 3, Definieren von Policies.

- **Logs:** Durch Klicken auf den Titel des Abschnitts wird in die Logs-Welt gewechselt. Dieser Abschnitt enthält Symbole und Links zu Folgendem:
  - **Client-Logs –** klicken Sie hierauf, um Logs und Alarme von geschützten Clients anzuzeigen.
  - **Server-Logs –** klicken Sie hierauf, um SafeGuard PortProtector Server-Logs anzuzeigen.
  - **Datei-Logs –** klicken Sie hierauf, um Logs anzuzeigen, die Dateien verfolgen, die auf geschützte Clients geschrieben bzw. von ihnen gelesen wurden.
  - **Zuletzt angezeigt –** hier wird eine Liste der zuletzt angezeigten Abfragen angezeigt (Abfragen ohne Namen werden nicht angezeigt). Klicken Sie zur Ausführung auf die gewünschten Abfrage. Abfragen sind durch ein vorangestelltes **Q** gekennzeichnet.

Im Kapitel *Anzeigen von Logs*, finden Sie eine detaillierte Erläuterung zu Logs, Abfragen und Log-Management.

- **Clients:** Durch Klicken auf den Titel des Abschnitts wird in die Clients-Welt gewechselt. Dieser Abschnitt enthält Symbole und Links zu Folgendem:
  - **Suspendierungskennwort gewähren –** klicken Sie hierauf, um für einen Client ein Suspendierungskennwort zu gewähren. Auf diese Weise können Sie den SafeGuard PortProtector Schutz temporär auf dem Client aufheben, ohne SafeGuard PortProtector Client deinstallieren zu müssen.
  - **Client-Logs erfassen –** klicken Sie hierauf, um Logs von geschützten Clients sofort zu abzurufen, ohne auf den Ablauf des **Intervalls** für den Logtransfer warten zu müssen.
  - **Client-Policy aktualisieren –** klicken Sie hierauf, um die Policies auf Clients sofort zu aktualisieren, ohne auf den Ablauf des vordefinierten Aktualisierungsintervalls warten zu müssen.

Im Kapitel *Verwalten von Clients*, finden Sie eine detaillierte Erläuterung der Client-Verwaltung.

- **Extras:** Dieser Abschnitt enthält Symbole und Links zu Folgendem:
  - **Allgemeine Policy-Einstellungen ändern –** klicken Sie hierauf, um das Fenster Allgemeine Policy-Einstellungen zu öffnen, in dem Sie allgemeinen Policy-Einstellungen ändern können. Dabei handelt es sich um die Standardeinstellungen für alle Policies, sofern keine policy-spezifischen Einstellungen definiert wurden. In *Schritt 9: Allgemeine Policy-Einstellungen definieren* in *Kapitel 3*, *Definieren von Policies*, finden Sie eine detaillierte Erläuterung.
  - **Administrationseinstellungen ändern –** klicken Sie hierauf, um das Fenster Administration zu öffnen, in dem Sie die Administrationseinstellungen ändern können.
  - **SafeGuard PortAuditor starten –** klicken Sie hierauf, um das Fenster Pfad zum SafeGuard PortAuditor zu öffnen, in dem Sie SafeGuard PortAuditor starten und Ihr Organisationsnetz scannen können, um aktuell und zuvor angeschlossene Geräte und WiFi-Links zu erkennen. Eine detaillierte Erläuterung finden Sie im SafeGuard PortAuditor Benutzerhandbuch.

### Status

Dieser Bereich in der unteren Hälfte des Fensters zeigt Informationen zu Ihrer SafeGuard PortProtector-Datenbank und Lizenz an. Der Bereich ist in zwei Abschnitte unterteilt, wie nachfolgend beschrieben:

- **Datenbank –** für jeden Logtyp (Client, File, Server) wird die Anzahl gespeicherter Tage angezeigt. Durch Klicken auf den Link **Pflegen** oder auf den Titel des Abschnitts wird in das Fenster *Datenbank-Management* gewechselt, in dem Sie die Einstellungen für die Tiefe und andere Einstellungen bei Bedarf ändern können. Falls in einem Notfall die Datensätze in der Datenbank gelöscht werden müssen (siehe *Definieren der Datenbankpflege-Einstellungen* in *Kapitel 8, Administration)*, wird in diesem Abschnitt eine Meldung angezeigt.

### Taskleiste

Die Taskleiste unten in der Start-Welt und allen anderen Welten zeigt den Namen des derzeit angemeldeten Administrators und den Namen des SafeGuard PortProtector Management Servers an.

# 3 Definieren von Policies

## Über dieses Kapitel

Dieses Kapitel beschreibt, wie SafeGuard PortProtector-Policies in der Policies-Welt erstellt und verwaltet werden. Es enthält die folgenden Abschnitte:

- ***Was ist eine Policy*** beschreibt, was eine Policy ist und wie sie Ihre Endpunkte schützt.
- ***Kurze Übersicht über die Policies-Welt*** beschreibt das Fenster der Policies-Welt.
- ***Definieren von SafeGuard PortProtector – Workflow*** liefert eine Übersicht über den Workflow zum Definieren einer neuen Policy. Dabei wird ein einfacher und klarer Vorgang zur Durchführung dieser Schritte beschrieben. Sie können bei Bedarf von diesem Verfahren abweichen. Jeder dieser Schritte verweist zu einem Unterabschnitt, in dem eine detailliertere Beschreibung zu finden ist.
- ***Freigeben von Geräten und WiFi-Verbindungen*** beschreibt, wie Sie in den Fenster *Device Control*, *Storage Control* und *WiFi Control* Gruppen von Gerätemodellen, Gruppen von spezifischen Geräten und Gruppen von WiFi-Netzen sowie deren Zugriffsberechtigungen auf die im Fenster *Port Control* zugelassenen Ports definieren.
- ***Freigeben von CD/DVD-Medien*** beschreibt, wie die Nutzung von mit Fingerprint versehenden CD/DVD-Medien zugelassen wird, indem Sie diese in eine White List eintragen.
- ***Verwalten von Policies*** erläutert, wie Sie Aktionen ausführen, wie etwa Speichern und Veröffentlichen einer Policy, Exportieren und Importieren von Policies, Löschen von Policies etc.
- ***Optionen für aktives Fenster*** behandelt das Duplizieren, Lösen und Schließen eines Fensters.

## 3.1 Was ist eine Policy

Eine SafeGuard PortProtector-Policy definiert, wie Sie den Zugang über die Ports der Endpunkte, die zu einer bestimmten Organisationseinheit (OU, Gruppe von Computern oder Benutzern) gehören, schützen möchten Die Gesamtheit der SafeGuard PortProtector-Policies und deren Zuweisung zu den Organisationseinheiten bestimmt die Schutzpolicy Ihrer Organisation.

Eine SafeGuard PortProtector-Policy gibt an, welche Ports zugelassen, gesperrt oder eingeschränkt werden. **Eingeschränkt** (Restricted) bedeutet, dass nur angegebene Gerätetypen, Gerätemodelle, spezifische Geräte oder WiFi-Verbindungen Zugang über diesen Port erlangen können.

In einer Policy werden die Zugriffsberechtigungen für Speichergerätetypen, Speichergerätemodelle und spezifische Speichergeräte sowie auch für WiFi-Verbindungen angegeben. Dabei können Sie festlegen, ob sie zugelassen, gesperrt oder eingeschränkt (wie für Geräte) oder mit schreibgeschütztem Zugriff zugelassen sind.

Eine Policy kann auch **Hardware-Keylogger** sperren, die an einen USB- oder PS/2-Port angeschlossen wurden. Hardware-Keylogger sind Geräte, die in feindlicher Absicht von Dritten zwischen eine Tastatur und den zugehörigen Hostcomputer geschaltet wurden, um Tastatureingaben zu protokollieren. Mit Ihrer Policy können Sie festlegen, ob Hardware-Keylogger gesperrt werden sollen, wenn sie von SafeGuard PortProtector entdeckt werden.

SafeGuard PortProtector-Policies können auch für jeden Port, jedes Gerät, jedes Speichergerät und jeden WiFi-Anschluss definieren, ob die Aktivitäten (wie etwa Anschließen oder Entfernen eines Geräts) protokolliert werden und ob diese Aktivitäten einen Alarm auslösen. Logs und Alarme werden verschlüsselt, auf dem SafeGuard PortProtector Management Server gespeichert und können in der Logs-Welt angezeigt werden, wie in *Kapitel 5, Anzeigen von Logs*, beschrieben. Alarme werden sofort an vordefiniert Ziele gesendet und können auch in der Logs-Welt angezeigt werden.

Die Dateitypkontrolle bietet eine weitere Ebene für die Überwachung der Aktivitäten in Ihrer Organisation, indem Sie eine versteckte Kopie der auf Wechselmedien bzw. CD/DVD geschriebenen oder davon gelesenen Dateien kontrollieren, einen Alarm bzw. ein Log erzeugen oder diese Dateien speichern können. Auch Datei-Logs können in der Logs-Welt angezeigt werden.

Bei der Integration mit einer Lösung zur Inhaltsprüfung eines Drittanbieters können Sie Dateien, die auf Speichergeräte übertragen werden, vor ihrer Übertragung überprüfen lassen.

Eine Policy kann so eingerichtet werden, dass Wechselmediengeräte, einschließlich der an einem durch diese Policy geschützten Computer angeschlossenen CD/DVD- und externen Festplatten, verschlüsselt werden, so dass nur von der Organisation verschlüsselte Geräte benutzt werden können. Die von der Organisation verschlüsselten Geräte können nur von Computern der Organisation benutzt werden. Dadurch wird ein Durchsickern von Unternehmensdaten verhindert. (Bei Bedarf gibt es Ausnahmen zu dieser Regel, siehe *Offline-Zugriff auf verschlüsselte Geräte* in *Kapitel 9, Endbenutzer-Erfahrung*).

In der Policy werden auch Einstellungen wie die Häufigkeit, mit der Logs von den SafeGuard PortProtector Clients zum Management Server gesendet werden, sowie der Text der Endbenutzer-Meldungen etc. definiert.

Sie können eine Policy auf jede Organisationseinheit anwenden, die in Ihrem Active Directory oder Novell eDirectory definiert ist.

SafeGuard PortProtector verfolgt einen positiven Sicherheitsansatz. Das bedeutet, dass alle Geräte gesperrt sind, sofern Sie keine Policy definieren, die deren Zugriff erlaubt.

In den folgenden Abschnitten wird beschrieben, wie Sie eine Policy definieren.

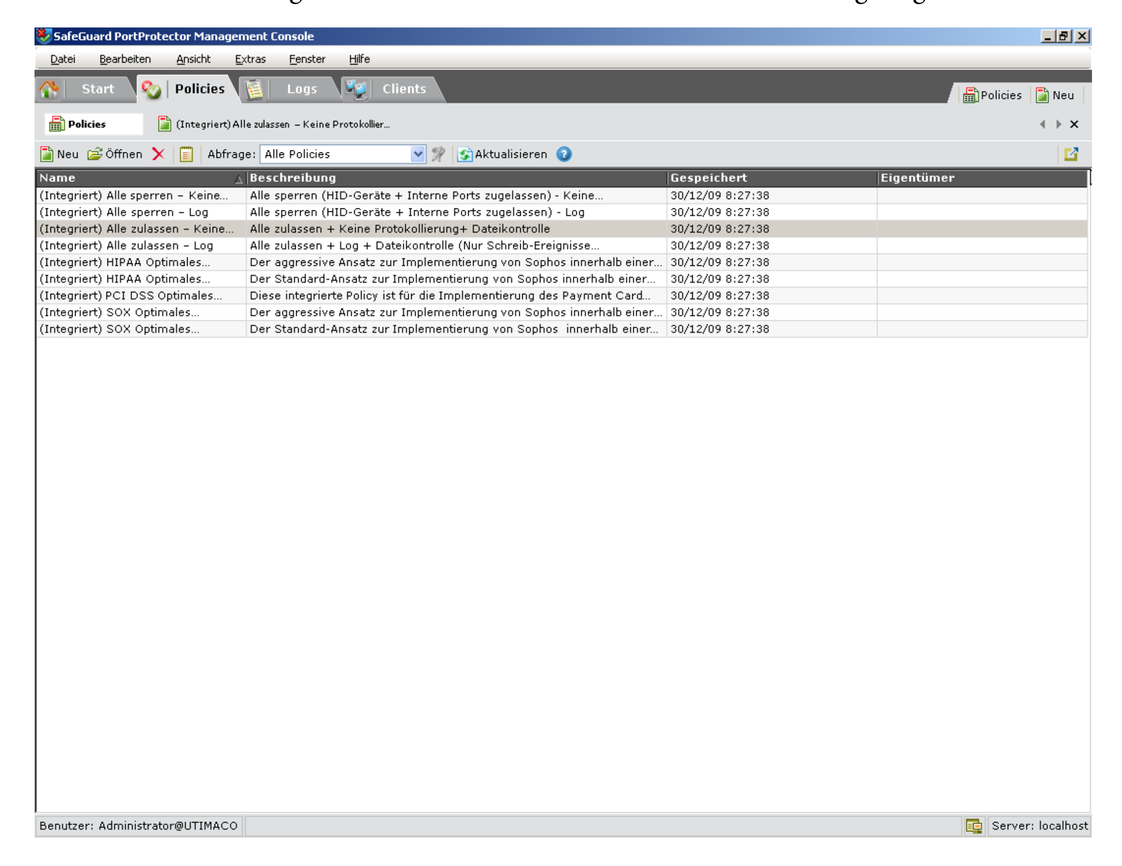
Die Policies schützen die Endpunkte in Ihrer Organisation sobald sie an die Computer in Ihrer Organisation verteilt wurden, wie in *Kapitel 4, Verteilen von Policies*, beschrieben.

Bevor wir mit der Definition von Policies beginnen, schauen wir uns kurz die Policies-Welt an und besprechen das Policy-Management.

## 3.2 Kurze Übersicht über die Policies-Welt

**So öffnen Sie die Policies-Welt:**

Klicken Sie auf die Registerkarte **Policies**. Das Fenster Policies wird angezeigt:




Das Fenster der Policies-Welt enthält die Abschnitte und Steuerungsschaltflächen, die in Übersicht über die Anwendung im Kapitel *Erste Schritte*, beschrieben wurden. Die Startschaltflächen und einige der Menüoptionen sind speziell für die Policies-Welt.

### 3.2.1 Startschaltflächen

Die spezifischen Startschaltflächen in der Policies-Welt sind:

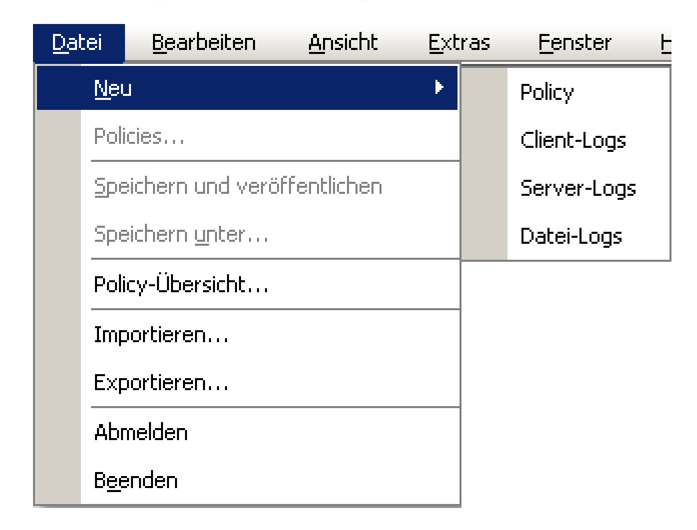
- **Policies** Policies – durch Klicken auf diese Schaltfläche wird das Fenster *Policies* geöffnet, in dem Sie Ihre Policies verwalten können.
- **Neu** Neu – durch **Klicken** auf diese Schaltfläche wird ein neues, unbenanntes Policy-Fenster geöffnet.

## 3.2.2 Menüs

Einige der Menüoptionen in der Policies-Welt sind speziell für diese Welt. Nachstehend finden Sie eine Beschreibung der einzelnen Menüs und der Optionen.

### 3.2.2.1 Menü Datei

Im Menü *Datei* in der Policies-Welt können Sie andere Welt-Fenster öffnen, Policies speichern, Policies exportieren und importieren etc.



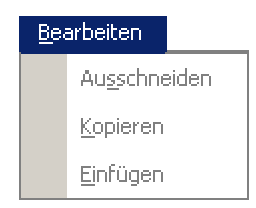

Das Menü *Datei* enthält folgende Optionen:

| Option | Beschreibung |
|---|---|
| **Neu** | Öffnet ein Untermenü, über das Sie ein neues Policy-Fenster, ein neues Client Log-Fenster, ein neues Server Log-Fenster oder ein neues File Log-Fenster öffnen können. |
| **Policies** | Ermöglicht Ihnen das Verwalten der Policies. |
| **Speichern und Veröffentlichen** | Speichert und veröffentlicht die Policy. |
| **Speichern unter** | Speichert die Policy unter einem neuen Namen und veröffentlicht sie. |
| **Policy-Übersicht** | Zeigt alle Policy-Informationen in einem einzelnen Fenster und in druckbarer Form. |
| **Importieren** | Importiert eine exportierte Policy. |
| **Exportieren** | Exportiert die Policy in eine externe Datei. |

| Option | Beschreibung |
|---|---|
| **Abmelden** | Meldet den aktuellen Benutzer von der Management Console ab. |
| **Beenden** | Meldet den aktuellen Benutzer ab und schließt die SafeGuard PortProtector Management Console. |

### 3.2.2.2 Menü Bearbeiten

Das Menü *Bearbeiten* umfasst die Optionen **Ausschneiden**, **Kopieren** und **Einfügen** für die Option **Gerät hinzufügen, Speichergerät hinzufügen** oder **WiFi-Netzwerk hinzufügen** (siehe auch die Beschreibung in *Freigeben von Geräten und WiFi-Verbindungen*). In anderen Fällen ist es deaktiviert.




### 3.2.2.3 Menü Ansicht

Über das Menü *Ansicht* können Sie das Fenster Policies aktualisieren, das eine Liste Ihrer Policies anzeigt, und den Fortschritt von Client-Tasks anzeigen lassen.




Das Menü *Ansicht* enthält folgende Optionen:

| Option | Beschreibung |
|---|---|
| **Aktualisieren** | Aktualisiert die Liste der Policies, so dass sie auf dem neuesten Stand ist. |
| **Client-Tasks** | Zeigt den Verlauf der Client-Tasks (weitere Informationen finden Sie in *Verfolgen des Fortschritts von* Client-Tasks in *Kapitel 6, Verwalten von Clients*). |

### 3.2.2.4 Menü Extras

Das Menü *Extras*, das bei allen Welten gleich ist, ist in *Menü* im Kapitel *Erste Schritte*, beschrieben.

#### 3.2.2.5 Menü Fenster

Das Menü *Fenster*, das bei allen Welten gleich ist, ist in *Menü* im Kapitel *Erste Schritte*, beschrieben.

#### 3.2.2.6 Menü Hilfe

Das Menü *Hilfe*, das bei allen Welten gleich ist, ist in *Menü* im Kapitel *Erste Schritte*, beschrieben.

### 3.2.3 Symbolleiste

Die Symbolleiste der Policies-Welt bietet schnellen Zugriff auf häufig genutzte Funktionen. Sie wird unterhalb der Menüleiste angezeigt und enthält die folgenden Schaltflächen:



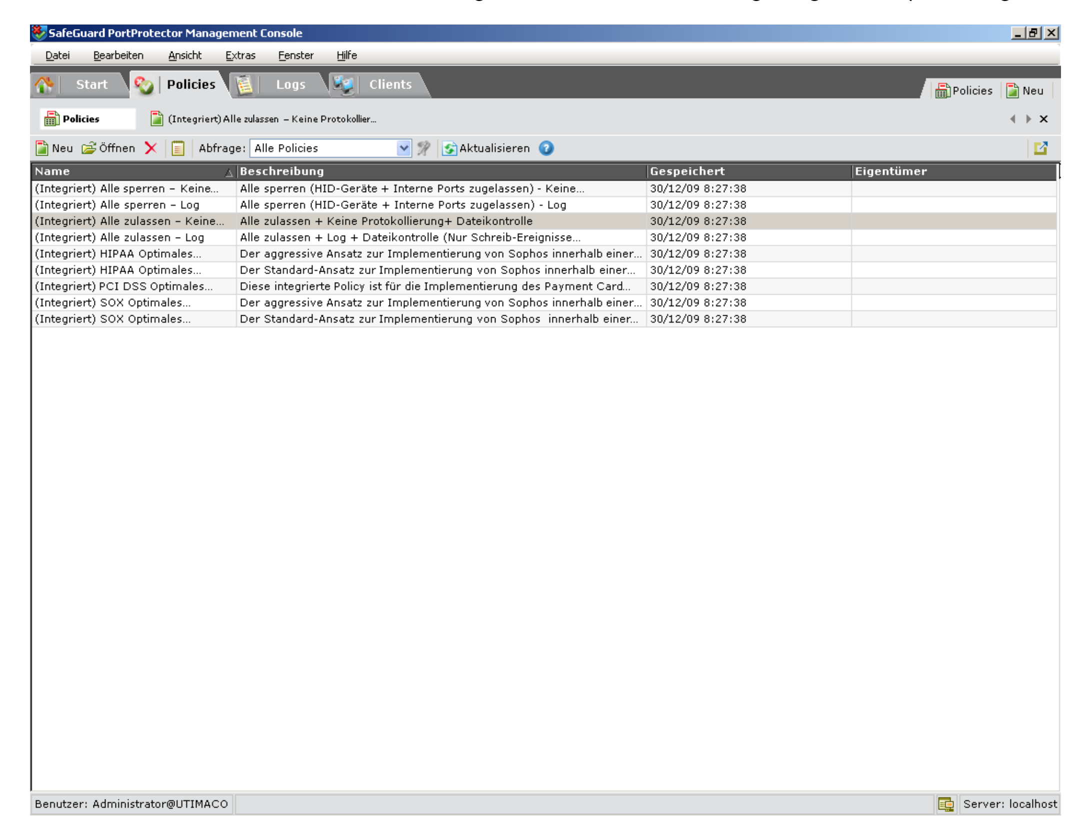

Nachfolgend eine kurze Beschreibung der einzelnen Schaltflächen in der Symbolleiste:

| Schaltfläche | Beschreibung |
| --- | --- |
| **Neu** | Öffnet eine neue Policy. |
| **Öffnen** | Öffnet die ausgewählte Policy. |
| **Delete** | Löscht die ausgewählte Policy. |
| **View Summary** | Zeigt alle Policy-Definitionen in einem einzelnen Fenster und in druckbarer Form. |
| **Aktualisieren** | Aktualisiert die Liste der Policies, so dass sie auf dem neuesten Stand ist. |
| **Hilfe** | Zeigt die Kontexthilfe des aktiven Fensters und ermöglicht den Zugriff auf andere Hilfethemen. |

**Hinweis:** Diese Symbolleiste wird im Fenster *Policies* angezeigt, in dem Sie die Policies verwalten können. Im Fenster Policy, in dem Sie die Policy-Eigenschaften definieren, ist eine andere Symbolleiste verfügbar, wie in *Schritt 4: Portkontrolle definieren* beschrieben.

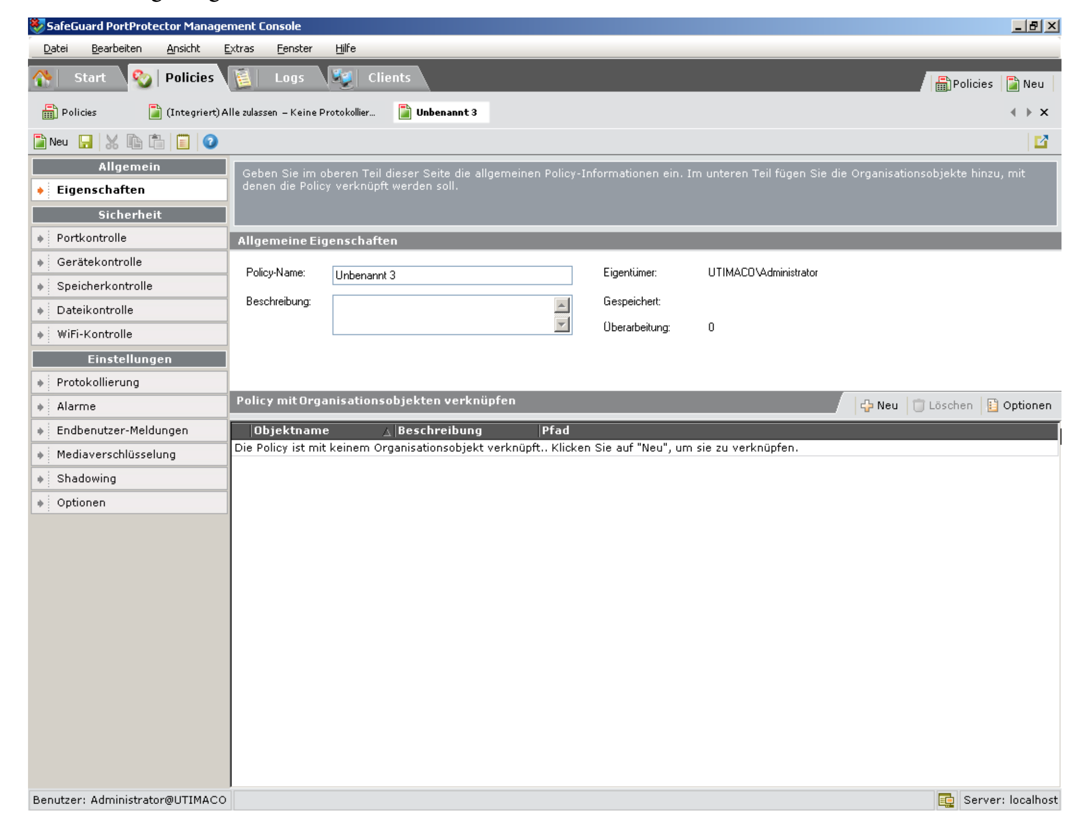
### 3.2.4 Arbeitsbereich

Im Arbeitsbereich wird standardmäßig das Fenster *Policies* angezeigt (Policy-Management):




Dieses Fenster kann jederzeit geschlossen bzw. geöffnet werden.

Wenn Sie eine Policy öffnen (ganz gleich, ob eine neue oder vorhandene), wird folgendes Fenster angezeigt:



Die linke Seite des Fensters enthält die folgenden Abschnitte:

- **Allgemein:** In diesem Abschnitt geben Sie den Namen und die Beschreibung der Policy ein und verknüpfen diese mit Organisationsobjekten. In *Verteilen von SafeGuard PortProtector Policies direkt vom Management Server aus* in *Kapitel 4, Verteilen von Policies*, finden Sie eine Erklärung dieses Abschnitts.
- **Sicherheit:** Dieser Abschnitt enthält die Definitionen der Sicherheitseinstellungen der Policy (Portkontrolle, Gerätekontrolle, Speicherkontrolle, **Dateikontrolle** und WiFi-Kontrolle). Diese Definitionen werden später in diesem Kapitel beschrieben.
- **Einstellungen:** Dieser Abschnitt enthält die Definitionen der zusätzlichen Einstellungen der **Policy** (Protokollierungen, Alarme, Endbenutzer-Meldungen, Verschlüsselung und Policy-Optionen). Diese Definitionen werden später in diesem Kapitel beschrieben.

Auf der rechten Seite, dem Hauptteil des Arbeitsbereichs, werden die verschiedenen Inhaltsarten angezeigt, die davon abhängen, was Sie im Abschnitt **Allgemein**, **Sicherheit** oder **Einstellungen** auf der linken Seite des Fensters ausgewählt haben.

Wenn alle Fenster geschlossen sind, ist der Arbeitsbereich leer. Sie können das Fenster *Policies* oder eine bestimmte Policy öffnen, indem Sie auf eine der Startschaltflächen




oben rechts im Fenster klicken.

Weitere Informationen zum Policy-Management finden Sie in *Verwalten von* Policies.

Weitere Informationen zum Definieren von Policies finden Sie in *Schritt 3: Policy erstellen*.

## 3.3 Definieren von SafeGuard PortProtector-Policies – Workflow

Im Folgenden finden Sie eine Übersicht über den Workflow zum Definieren einer neuen Policy. Jeder dieser Schritte verweist zu einem Unterabschnitt, in dem eine detailliertere Beschreibung zu finden ist.

In diesem Workflow wird ein einfacher und klarer Vorgang zur Durchführung dieser Schritte beschrieben. Sie können bei Bedarf von diesem Verfahren abweichen.

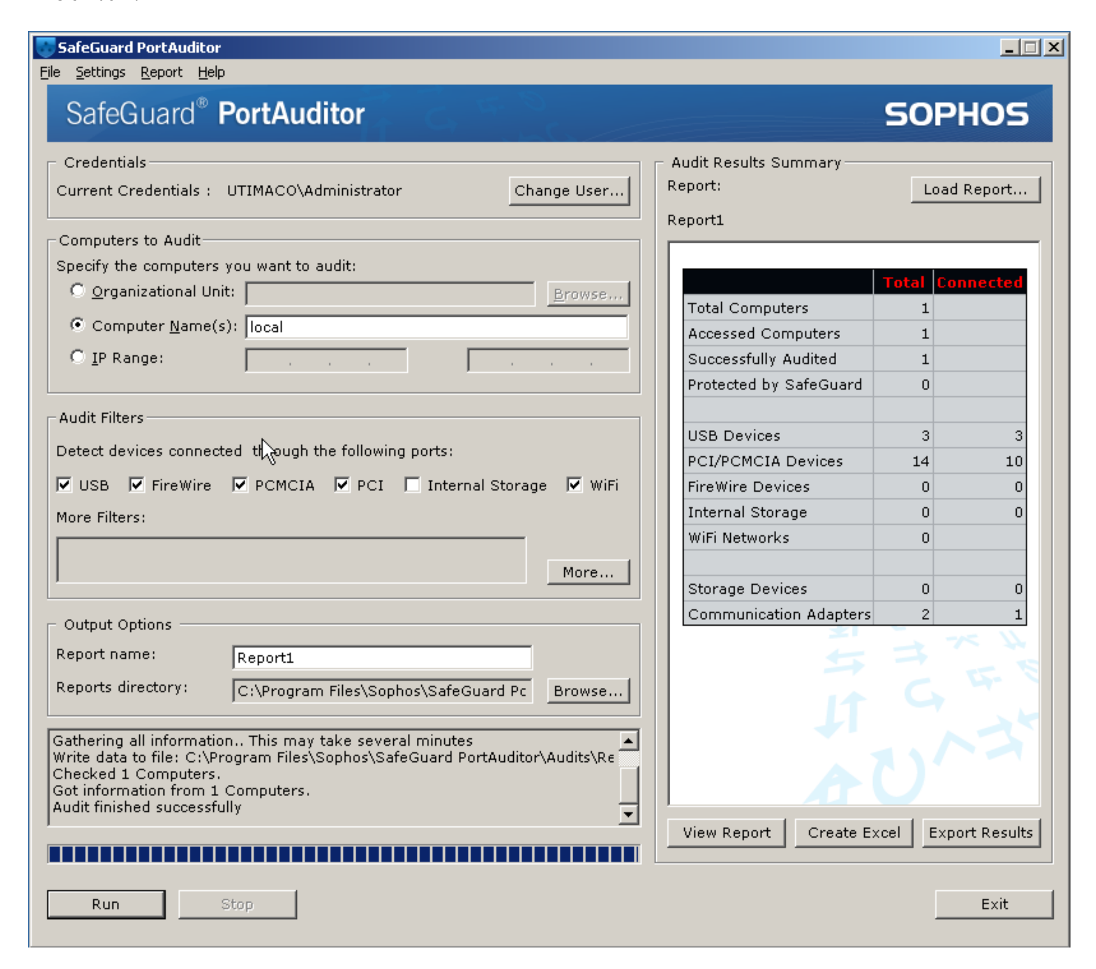
- ***Schritt 1: Computer scannen und Port-/Geräte-/WiFi-Nutzung erkennen:*** *Verwenden Sie SafeGuard PortAuditor*, um die Computer in Ihrem Netz zu scannen und so die Geräte und WiFi-Netze zu erkennen, die derzeit angeschlossen sind bzw. früher angeschlossen waren (in der Registry des Computers angegeben), wie im SafeGuard PortAuditor Benutzerhandbuch beschrieben Diese Informationen ziehen Sie bei der Definition einer Policy zu Rate, um einfach anzugeben, welche Ports und Geräte zugelassen, gesperrt, eingeschränkt oder schreibgeschützt zugelassen werden.
- ***Schritt 2: Policy planen*** beschreibt die Informationen, die Sie für die richtige Planung der besten Policy für den Schutz der Endpunkte in Ihrer Organisation erfassen sollten.
- ***Schritt 3: Policy erstellen*** beschreibt die Erstellung einer neuen Policy. Sie können so beliebig viele Policies erstellen – eine für Ihre gesamte Organisation oder verschiedene Policies, jeweils eine für jede Computer- oder Benutzergruppe.
- ***Schritt 4: Portkontrolle definieren*** beschreibt, wie die Portkontrolle in Ihrer Policy definiert wird, d. h. welche Ports zugelassen, welche gesperrt und welche auf die Nutzung durch bestimmte Geräte eingeschränkt werden. Bei der Portkontrolle können Sie außerdem Log- und Alarmoptionen für die Portinitialisierung und/oder -aktivitäten festlegen. Darüber hinaus wird in diesem Abschnitt beschrieben, wie eine Hybridnetzüberbrückung vermieden wird.
- ***Schritt 5: Gerätekontrolle definieren*** beschreibt, wie man noch detaillierter definiert, welche Geräte über eingeschränkte Ports an Ihren Endpunkten angeschlossen werden dürfen. Bei der Gerätekontrolle können Sie außerdem Log- und Alarmoptionen für die Geräteaktivitäten festlegen.
- ***Schritt 6: Speicherkontrolle definieren*** In diesem Schritt definieren Sie auch, ob die Daten auf Ihren internen Festplatten verschlüsselt werden oder nicht. Beschreibt, wie man noch detaillierter definiert, welche Speichergeräte an Ihre Endpunkte angeschlossen werden dürfen und welche nur im schreibgeschützten oder verschlüsselten Modus angeschlossen werden dürfen. Bei der Speicherkontrolle können Sie auch Log- und Alarmoptionen für alle Aktivitäten auf einem Speichergerätetyp, Gerätemodell oder spezifischen Speichergerät festlegen.
- ***Schritt 7: Dateikontrolle definieren*** beschreibt die Kontrolle von Dateien, die auf Speichergeräte geschrieben oder von ihnen gelesen werden, das Shadowing, Verfolgen bzw. Überprüfen ihrer Inhalte je nach Dateityp. Darüber hinaus können Sie Log- and Alarmoptionen für geschriebene und gelesene Dateien je nach Typ festlegen.
- ***Schritt 8: WiFi-Kontrolle definieren*** beschreibt, wie man definiert, welche WiFi-Verbindungen zugelassen werden. Außerdem wird beschrieben, wie Sie Log- und Alarmoptionen für die WiFi-Aktivitäten festlegen können

- ***Schritt 9: Allgemeine Policy-Einstellungen definieren*** beschreibt, wie Standardwert für die Einstellungen der Protokollierung, Endbenutzer-Meldungen und Optionen definiert werden, die weiter unten in den Schritten 10-16 beschrieben werden.
- ***Schritt 10: Protokollierung definieren*** beschreibt, wie Protokollierungseinstellungen für die aktuelle Policy definiert werden, wie etwa die Häufigkeit mit der Logeinträge von einem geschützten Endpunkt an SafeGuard PortProtector gesendet werden.
- ***Schritt 11: Alarme definieren*** beschreibt die Auswahl der Ziele für Alarme, die von einem durch diese Policy geschützten Endpunkt stammen.
- ***Schritt 12: Endbenutzer-Meldungen definieren*** beschreibt die Definition der Meldungen, die dem Endbenutzer vom SafeGuard PortProtector Client auf jedem Computer angezeigt werden.
- ***Schritt 13: Mediaverschlüsselung definieren*** beschreibt die Definition der Verschlüsselungseinstellungen, wenn die Policy eine Verschlüsselung verlangt, sowie das Verhalten des Endpunkts beim Versuch, auf ein nicht verschlüsseltes Gerät zuzugreifen, und die Zugriffsautorisierung auf ein verschlüsseltes Gerät, wenn es nicht an das Organisationsnetz angeschlossen ist.
- ***Schritt 14: Inhaltsprüfung definieren*** beschreibt die Definition bestimmter Einstellungen, die bei der Inhaltsprüfung benötigt werden, z. B. ob für als sensibel erkannte Dateien Alarme ausgegeben werden sollen. Dieser Schritt braucht nur dann ausgeführt zu werden, wenn Sie SafeGuard PortProtector mit einer Lösung zur Inhaltsprüfung eines Drittanbieters integrieren.
- ***Schritt 15: Einstellungen für Datei-Shadowing definieren*** beschreibt, wie Sie SafeGuard PortProtector-Einstellungen zur Rückverfolgung und zum Erfassen von Kopien von Dateien definieren, die zu/von externen Speichergeräten verschoben wurden.
- ***Schritt 16: Optionen definieren*** ermöglicht es Ihnen, die verschiedenen Verhaltensaspekte des SafeGuard PortProtector Client auf den Endpunkten zu definieren.
- ***Schritt 17: Policy-Berechtigungen definieren*** beschreibt, wie definiert wird, für welche Administratoren die Policy sichtbar sein wird, wenn Sie die Verwaltungsmöglichkeit auf der Basis von Safend Protector Domain Partition gewählt haben.
- ***Schritt 18: Policy speichern und veröffentlichen*** beschreibt die Optionen für das Speichern der Policy in der Policy-Datenbank und ihrer Veröffentlichung, so dass sie mit den relevanten Clients verknüpft werden kann.

Sobald SafeGuard PortProtector Policies an die SafeGuard PortProtector Clients verteilt und angewandt wurden, implementieren sie Ihre Schutzpolicy auf jedem Computer. In *Kapitel 4, Verteilen von Policies* finden Sie eine Beschreibung, wie SafeGuard PortProtector-Policies an die Endpunkte Ihrer Organisation verteilt werden.

## 3.3.1 Schritt 1: Computer scannen und Port-/Geräte-/WiFi-Nutzung erkennen

Auch wenn SafeGuard PortAuditor kein integraler Bestandteil von SafeGuard PortProtector ist, geht dieses Tool doch mit SafeGuard PortProtector Hand in Hand und ergänzt das System mit einer kompletten Sicht darauf, welche Ports, Geräte und Netze von den Benutzern in Ihrer Organisation genutzt werden (oder früher genutzt wurden). Mit Hilfe eines SafeGuard PortAuditor-Scans können Sie die Geräte und Netze auswählen, deren Nutzung Sie genehmigen möchten.




Sie können SafeGuard PortAuditor aus SafeGuard PortProtector heraus starten, wie in *Auditing von Geräten in Kapitel 6, Verwalten von Clients, beschrieben.* Weitere Informationen finden Sie im *SafeGuard PortAuditor Benutzerhandbuch.*

## 3.3.2 Schritt 2: Policy planen

Bevor Sie mit der Definition Ihrer Policy beginnen, sollten Sie sich etwas Zeit für die Planung einer Policy nehmen, die sich für Ihre Organisation am besten eignet. Die beste SafeGuard PortProtector-Policy für Ihre Organisation zeichnet sich dadurch aus, dass sie den Sicherheitsbedürfnissen gerecht wird und dennoch die Anforderungen der Personen erfüllt, die Zugang über die Ports der Computer in Ihrer Organisation benötigen.

Als Erstes sollten die Arten der Gruppen der Organisationseinheiten (OU) geplant werden, für die die Policies gelten sollen.

### 3.3.2.1 Benutzer- und Computer-Policies

Standardmäßig verwendet SafeGuard PortProtector Einstellungen für Benutzer-und Computergruppen, die von Active Directory kontrolliert werden. Jede Option hat ihren Vorteil, wie nachfolgend beschrieben.

- **Für Benutzergruppen:** Wenn Sie Ihre Policies für Benutzergruppen definieren, können Sie die Berechtigungen für die einzelnen Benutzer detaillierter angeben.
- **Für Computergruppen:** Die Definition Ihrer Policies für Computer ermöglicht Ihnen den Schutz der Endpunkte der Computer in Ihrer Organisation unabhängig vom angemeldeten Benutzer.
  ***Policies, die für Benutzer gelten, überschreiben solche Policies, die für Computer gelten:***

SafeGuard PortProtector setzt die Policies wie folgt durch: Zunächst wird eine Benutzer-Policy angewendet, sofern eine für den derzeit angemeldeten Benutzer vorliegt. Andernfalls sucht SafeGuard PortProtector nach einer Policy, die dem Computer zugeordnet ist, und nutzt diese, sofern vorhanden. Das bedeutet: Wenn kein Benutzer angemeldet ist, wird die computerspezifische Policy angewandt. Deshalb ist es ratsam, die benutzerbezogenen Policies zu verteilen, so dass ein Benutzer dieselbe Policy erhält, ganz gleich an welchem Computer er angemeldet ist. Außerdem sollten computerspezifische Policies festgelegt werden, die mehr Einschränkungen enthalten. Diese computerspezifischen Policies sollten dennoch Zugriff auf Geräte wie Maus und Tastatur zulassen, damit sie genutzt werden können, wenn kein Benutzer oder ein Benutzer von außerhalb der Domäne angemeldet ist.

Bei der Erstkonfiguration des SafeGuard PortProtector Clients werden alle Port- und Geräteaktivitäten zugelassen, d. h. nichts ist gesperrt. Eine Konfiguration mit Berechtigungen ist erforderlichen, damit nicht alle Portaktivitäten automatisch direkt nach der Installation von SafeGuard PortProtector Client blockiert werden.

Das bedeutet: Bis Sie tatsächlich Policies definieren und an Ihre Endpunkte verteilen (für Benutzer oder für Computer), läuft der Computer, auf dem SafeGuard PortProtector Client gerade installiert wurde, wie zuvor weiter (ohne Sperrung von Ports und Geräten).

**Hinweis:** Wenn eine Policy auf dem Endpunkt manipuliert wird, ruft SafeGuard PortProtector sofort einen Panikmodus auf, der den gesamten Zugriff auf Ports und Geräte sperrt.

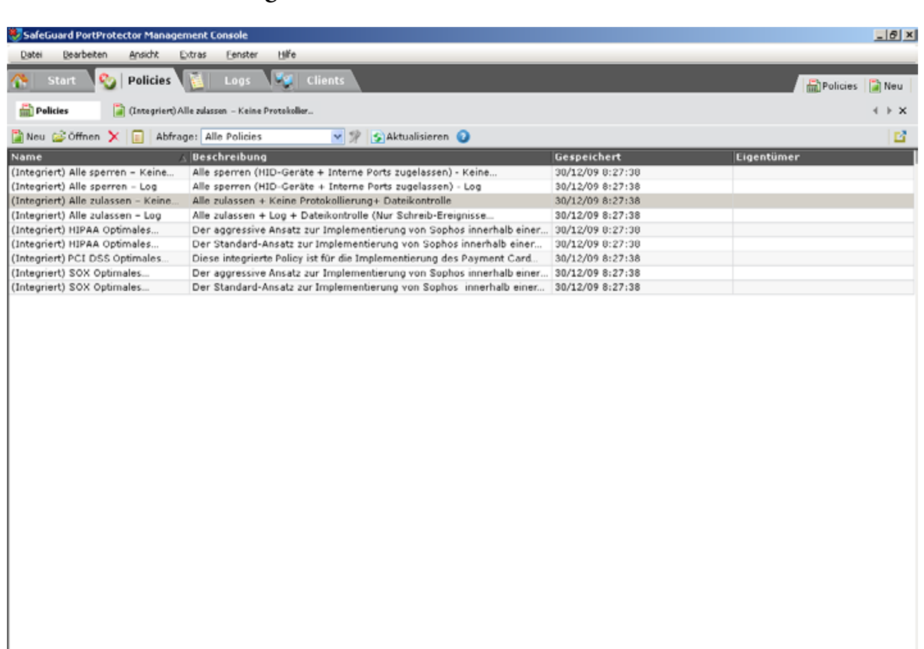
## 3.3.3 Schritt 3: Policy erstellen

Dieser Abschnitt beschreibt, wie Sie eine neue Policy in der Policies-Welt erstellen. Sie können mit den Standardeinstellungen oder mit einer Vorlage (in *Policy-Vorlage* in *Kapitel 8, Administration*, beschrieben) beginnen oder eine vorhandene Policy als Ausgangspunkt benutzen.

SafeGuard PortProtector wird mit mehreren integrierten Policies geliefert, die Sie bei Bedarf als Ausgangsbasis benutzen können. Dazu gehören:

- **(Integriert) Alle zulassen – Keine Protokollierung:** Alle Geräte und Dateien sind zugelassen, es erfolgt keine Protokollierung.
- **(Integriert) Alle zulassen + Log:** Alle Geräte und Dateien sind zugelassen, die **Geräteaktivitäten** werden protokolliert, geschriebene Dateien werden protokolliert**.**
- **(Integriert) Alle sperren – Keine Protokollierung:** Alle Geräte außer HDI-Geräten sind gesperrt, es **erfolgt** kein Protokollierung.
- **(Integriert) Alle sperren + Log:** Alle Geräte außer HDI-Geräten sind gesperrt, die **Geräteaktivitäten** werden protokolliert, geschriebene Dateien werden protokolliert.

**Klicken Sie auf die Registerkarte *Policies***, um die Policies-Welt zu öffnen.




Es gibt mehrere Ansätze, mit einer neuen Policy zu beginnen:

- **Von den Standardwerten oder eine Vorlage aus:** Wenn Sie eine neue Policy öffnen, werden im Fenster Policy die voreingestellten Policy-Definitionen des Systems angezeigt.
- **Auf der Basis einer vorhandenen Policy:** Wenn Sie bereits Policies über die Management Server Console definiert haben, können Sie diese Definitionen als **Grundlage** für eine neue Policy verwenden, indem Sie die vorhandene Policy duplizieren oder sie unter einem anderen Namen speichern.
- **Auf der Basis einer Policy-Vorlage:** Sie können auch eine Policy-Vorlage definieren, die dann anstelle der Standardwerte als Grundlage für neue Policy-Definitionen dient (siehe *Policy-Vorlage* im Kapitel *Administration*).

#### 3.3.3.1 Erstellen einer neuen Policy

Dieser Abschnitt erläutert, wie Sie eine neue Policy von Grund auf erstellen.

**So erstellen Sie eine neue Policy:**

Klicken Sie in der Policies-Welt oben rechts in der Registerkarte auf **Neu** ( Neu )

ODER

Klicken Sie in der Symbolleiste auf **Neu**

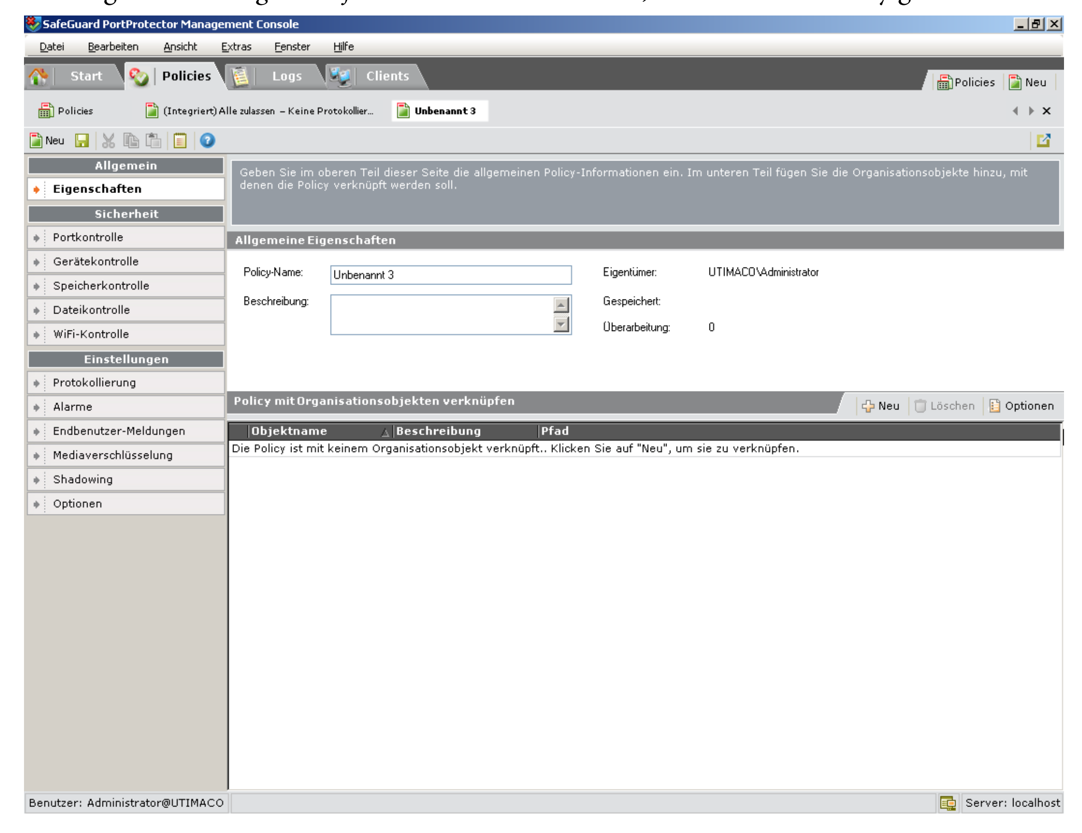
ODER

Klicken Sie in der Fensterleiste mit der rechten Maustaste auf eine Policy und wählen Sie **Neue Policy**

ODER

Wählen Sie im Menü *Datei* die Option **Neu.**

Die Registerkarte *Eigenschaften* wird mit einer neuen, unbenannten Policy geöffnet:




##### 3.3.3.1.1 Policy-Eigenschaften

In diesem Fenster können Sie den Namen und eine Beschreibung für die Policy eingeben. Eine neue Policy enthält die Standardwerte oder die Werte der Policy-Vorlage, sofern Sie eine solche Vorlage definiert haben (siehe *Policy-Vorlage* im Kapitel *Administration*).

#### 3.3.3.2 Erstellen einer neuen Policy aus einer vorhandenen Policy

Dieser Abschnitt erläutert, wie Sie eine neue Policy aus einer vorhandenen erstellen

**So erstellen Sie eine neue Policy von einer vorhandenen:**

1 Öffnen Sie die vorhandene Policy wie in *Verwalten* von *Policies* erläutert, und ändern Sie diese nach Bedarf ab.

2 Wählen Sie im Menü *File* die Option **Speichern unter**, und speichern Sie sie unter einem neuen Namen.

Alternativ können Sie eine vorhandene Policy duplizieren und sie unter einem neuen Namen speichern, wie in *Fenster duplizieren* in *Kapitel 2, Erste Schritte*, erläutert.

Die folgenden Schritte erläutern, wie Sie Ihre Policy definieren und speichern.

### 3.3.4 Schritt 4: Portkontrolle definieren

In diesem Schritt werden die Portberechtigungen und Berechtigungen für Hybridnetzüberbrückung festgelegt.

*Portberechtigungen*

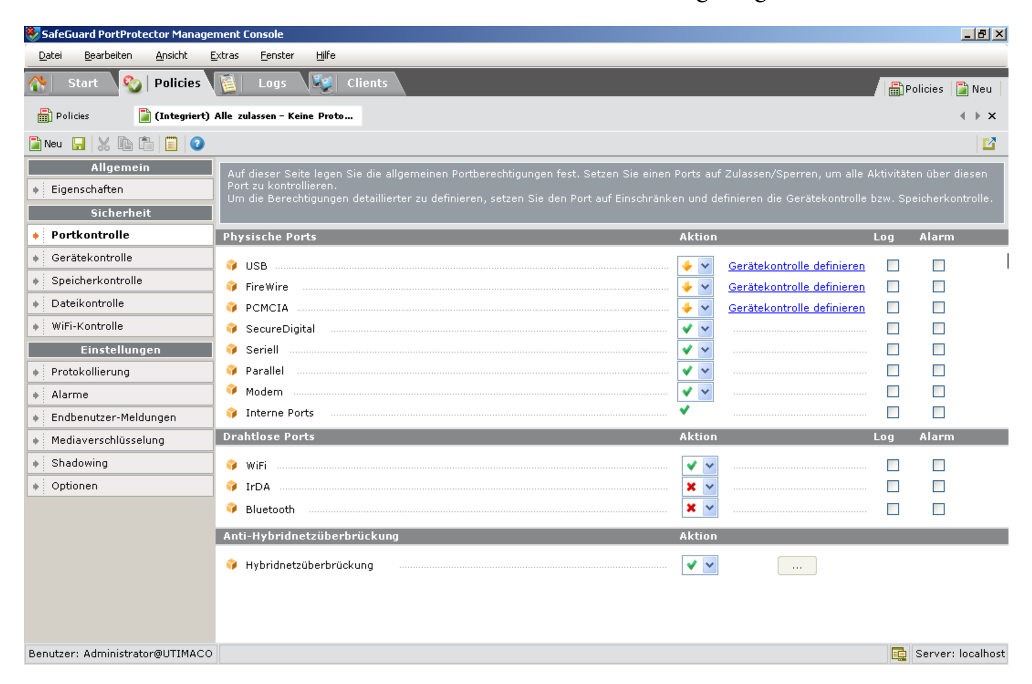
SafeGuard PortProtector ermöglicht eine positive Sicherheit, indem der Zugriff auf alle Ports auf allen Computern, an die eine Policy verteilt wurde, gesperrt wird, sofern die Policy nicht den Zugriff auf den Port zulässt. Sie können für jeden Port (USB, FireWire, PCMCIA, Secure Digital, seriell, parallel, Modem, WiFi, IrDA oder Bluetooth) Folgendes angeben:

- **Zulassen:** Diese Option legt fest, dass der Port zu jedem Zweck ohne Einschränkung auf diesem Kommunikationskanal genutzt werden kann.
- **Sperren:** Diese Option bedeutet, dass über diesen Port kein Zugriff erfolgen kann. Der Port ist nicht verfügbar, so als ob seine Kabel abgetrennt wären. Wenn ein Port gesperrt ist, können Sie festlegen, dass Versuche der Portinitialisierung protokolliert werden oder dass sie Alarme auslösen.
- **Einschränken:** Bei USB-, FireWire-, PCMCIA- und WiFi-Ports haben Sie auch die Möglichkeit, den Zugriff auf diese Porttypen als eingeschränkt zu definieren. Bei der Einstellung **Eingeschränkt** können Sie detaillierter (d. h. mit mehr Granularität) angeben, welche Geräte oder Verbindungen auf den Port zugreifen dürfen. Sie können z. B. angeben, dass nur USB-Geräte eines spezifischen **Modells** oder sogar nur bestimmte USB-Geräte (d. h. spezifische Geräte mit einer eindeutigen Seriennummer) zugelassen werden. Für physische Ports verwenden Sie hierfür die Option **Device Control**, die in *Schritt 5: Gerätekontrolle definieren* beschrieben ist, und die Option **Storage Control**, die in *Schritt 6: Speicherkontrolle definieren* beschrieben ist. Für drahtlose Ports verwenden Sie hierfür die Option **WiFi Control**, die in *Schritt 8: WiFi-Kontrolle definieren* beschrieben ist.

**Hinweis:** Die Aspekte der Gerätekontrolle und WiFi-Kontrolle einer Policy gelten nur für Ports mit Einschränkungen. Der Aspekt der Speicherkontrolle gilt sowohl für eingeschränkte als auch für zugelassene Ports.

**So definieren Sie die Portkontrolle:**

1 Öffnen Sie das Fenster *Portkontrolle*, indem Sie auf der linken Seite die Schaltfläche **Portkontrolle** im Menü *Sicherheit* wählen, wie unten gezeigt:




- Die Symbolleiste für die Anzeige oder Änderung einer Policy ist anders als die zuvor beschriebene Symbolleiste, die bei der Anzeige des ersten Fensters Policies erscheint:




Nachfolgend eine kurze Beschreibung der einzelnen Schaltflächen in der Symbolleiste:

| Schaltfläche | Beschreibung |
| --- | --- |
| **Neu** | Öffnet eine neue Policy. |
| **Speichern und veröffentlichen** | Speichert und veröffentlicht die Policy. |
| **Ausschneiden** | Entfernt eine Gruppe aus der Ausnahmenliste (in den Registerkarten Gerätekontrolle und Speicherkontrolle aktiviert, sobald der Ausnahmenliste Gruppen hinzugefügt wurden). |
| **Kopieren** | Kopiert eine Gruppe aus der Ausnahmenliste (in den Registerkarten Gerätekontrolle und Speicherkontrolle aktiviert, sobald der Ausnahmenliste Gruppen hinzugefügt wurden). |

| Schaltfläche | Beschreibung |
|---|---|
| **Einfügen** | Fügt eine Gruppe in die Ausnahmenliste ein (in den Registerkarten Gerätekontrolle und Speicherkontrolle aktiviert, wenn in der Ausnahmenliste eine Gruppe ausgeschnitten oder kopiert wurde). |
| **Policy-Zusammenfassung** | Zeigt alle Policy-Definitionen in einem einzelnen Fenster und in druckbarem HTML-Format. |
| **Hilfe** | Zeigt die Kontexthilfe des aktiven Fensters und ermöglicht den Zugriff auf andere Hilfethemen. |

- Über das Menü *Aktion* können Sie mit den Optionen Zugelassen oder Gesperrt angeben, ob ein Port zugelassen oder gesperrt ist. Für USB-, FireWire-, PCMCIA- und WiFi-Ports besteht mit der Option Eingeschränkt auch die Möglichkeit der Einschränkung.
- Mit Hilfe der *Log*-Kontrollkästchen können Sie angeben, ob Portinitialisierungen bzw. Portaktivitäten protokolliert und ob bei Portereignissen Alarme ausgelöst werden sollen.
- Mit Hilfe der *Alarm*-Kontrollkästchen können Sie angeben, ob bei Portereignissen Alarme ausgelöst werden sollen.

2 Geben Sie für jeden Port an, ob der Aktionstyp **Zulassen** ( ✔ ), **Sperren** ( ✖ ) oder **Einschränken** ( ⬇ ) ist, indem Sie die entsprechende Option aus der Dropdown-Liste im Menü *Aktion* wählen. Die Bedeutung der einzelnen Optionen wurde zu Beginn dieses Abschnitts beschrieben.

3 Wenn Sie im vorangegangenen Schritt für die USB-, FIREWIRE-, PCMCIA-Ports **Einschränken** gewählt haben, wird rechts neben der Dropdown-Liste der Link Gerätekontrolle definieren angezeigt. Das Fenster *Gerätekontrolle* kann über diesen Link oder durch Auswahl der Schaltfläche **Gerätekontrolle** im Menü *Sicherheit* geöffnet werden. Verwenden Sie eine dieser Möglichkeiten, um die Gerätemodelle oder spezifische Geräte zu definieren, denen Zugriff über diesen Port gewährt wird. Weitere Informationen finden Sie in *Schritt 5: Gerätekontrolle definieren*.

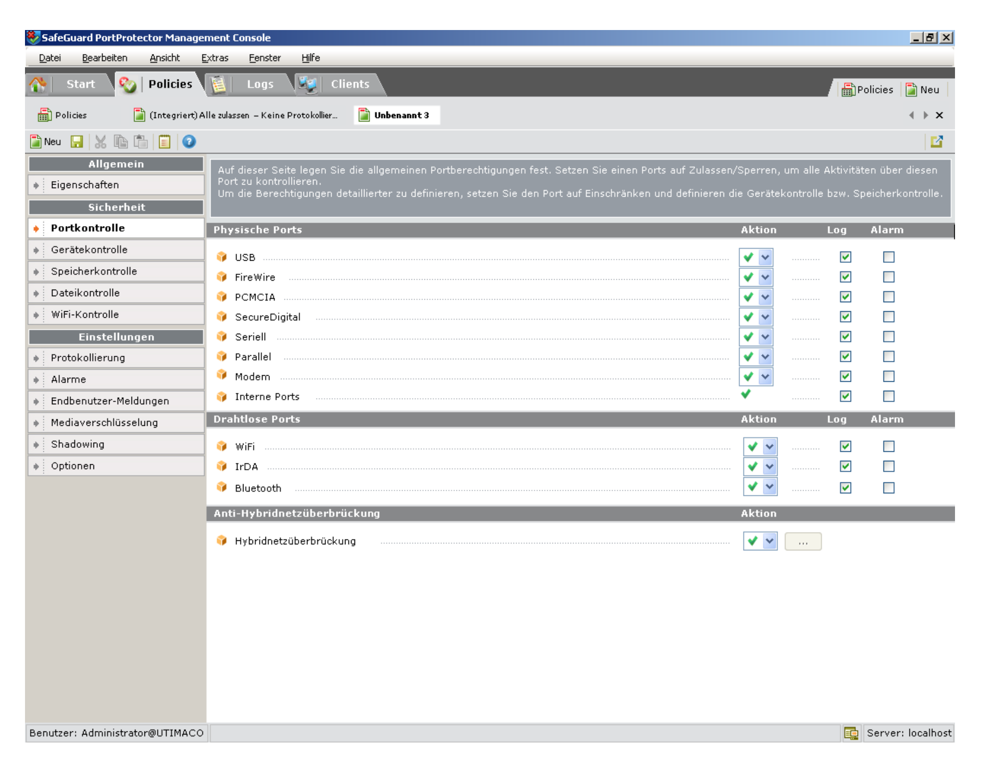
4 Wenn Sie im vorangegangenen Schritt für den WiFi-Port **Einschränken** gewählt haben, wird rechts neben der Dropdown-Liste der Link Define WiFi Control angezeigt. Das Fenster *WiFi Control* kann über diesen Link oder durch Auswahl der Schaltfläche **WiFi-Kontrolle** im Menü *Sicherheit* geöffnet werden. Verwenden Sie eine dieser Möglichkeiten, um die zugelassenen WiFi-Verbindungen zu definieren. Weitere Informationen finden Sie in *Schritt 5: Gerätekontrolle definieren*.

5 Geben Sie für jeden Port mit dem Kontrollkästchen **Log** an, ob eine Portinitialisierung für diesen Port protokolliert werden soll. Wenn dieses Kontrollkästchen markiert ist, wird bei jeder Initialisierung des Ports im SafeGuard PortProtector-Log ein Ereignis aufgezeichnet. Das gilt auch für interne Ports.

6 Geben Sie für jeden Port an, ob eine Portinitialisierung (zusätzlich zur Protokollierung) einen Alarm auslöst, indem Sie das Kontrollkästchen **Alarm** für diesen Port markieren. (Ein Alarm muss immer von einem Logeintrag begleitet sein. Deshalb wird automatisch auch das Kontrollkästchen **Log** markiert, sobald Sie das Kontrollkästchen **Alarm** markieren)

**Hinweis:** Anfangs, nach der Installation von SafeGuard PortProtector, möchten Sie vielleicht lieber eine der integrierten Policies verwenden (siehe *Schritt 3: Policy erstellen*). Alternativ können Sie eine Policy mit einem hohen Maß an Berechtigungen erstellen und verteilen, die den Zugriff auf alle Ports zulässt (nicht gesperrt oder eingeschränkt) und einfach die Aktivitäten protokolliert.

In diesem Fall setzen Sie die Ports auf **Zulassen** und markieren das Kontrollkästchen **Log** für jeden Port. Die Optionen bei **Port-Kontrolle** könnten dann folgendermaßen aussehen:




**Hinweis:** SafeGuard PortProtector überwacht auch **interne Computer-Ports.** Zu den internen Ports gehören Speicherbusse, wie etwa IDE, SCSI, ATA und S-ATA, für den Anschluss interner Festplatten sowie PCI und PCI-X genutzt werden, die Geräte wie Modems und Netzwerkkarten bedienen.
Bei **Interne Ports** ist *Aktion* immer auf **Zulassen** gesetzt, weil diese Ports zwar überwacht aber nicht kontrolliert werden können. Änderungen an diesen Ports können protokolliert werden, und es kann dafür ein Alarm ausgegeben werden. Dies ist beispielsweise bei folgenden Szenarien hilfreich: Ein cleverer, bösartiger Benutzer könnte eine zusätzliche Festplatte am internen IDE-Bus anschließen, um Firmendaten auf dieses Gerät zu ziehen, ohne eine Spur zu hinterlassen. Dank dieser Funktion können die Administratoren sofort bei jedem Anschließen oder Trennen von Geräten an den internen Ports der geschützten Endpunkte alarmiert werden.

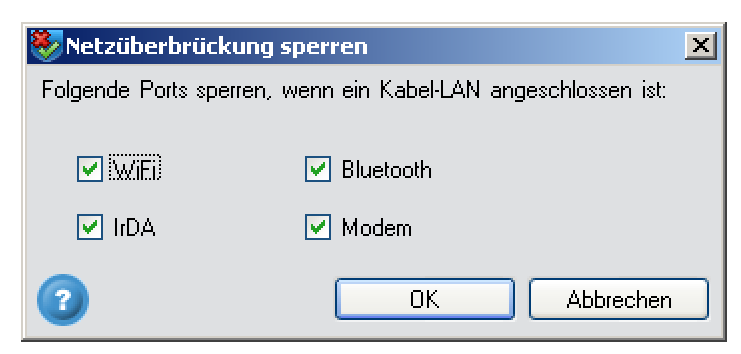
*Berechtigungen für Hybridnetzüberbrückung*

Mit SafeGuard PortProtector können Administratoren die Nutzung verschiedener Netzwerkprotokolle kontrollieren und die deren gleichzeitige Nutzung verhindern, was zu versehentlicher oder unbeabsichtigter Hybridnetzüberbrückung führen kann (z. B. WiFi-Bridging und 3G-Karten-Bridging). Wenn SafeGuard PortProtector Clients so konfiguriert werden, dass der Zugriff auf WiFi-, Bluetooth-, Modem- oder IrDA-Links blockiert wird während die verkabelte TCP/IP-Netzwerkschnittstelle mit einem Netz verbunden ist, können die Benutzer bestimmte Netzwerkprotokolle nur dann verwenden, wenn sie vom Netz getrennt sind. Auf diese Weise werden der Aufbau und der mögliche Missbrauch einer Hybridnetzbrücke vermieden.

Berechtigungen für Hybridnetzüberbrückung werden im Fenster *Netzüberbrückung sperren* festgelegt.

**So öffnen Sie das Fenster Block Network Bridging:**

Klicken Sie auf die Schaltfläche [...]. Das Fenster Netzüberbrückung sperren wird angezeigt:




Hier können Sie die Berechtigungen für eine Hybridnetzüberbrückung festlegen, wie *Blockieren der Hybridnetzüberbrückung* erläutert.

#### 3.3.4.1 Blockieren der Hybridnetzüberbrückung

Im Fenster *Netzüberbrückung sperren* definieren Sie, welche Wireless-Ports gesperrt werden sollen, wenn der Endpunkt mit dem verkabelten LAN verbunden ist.

**So sperren Sie die Hybridnetzüberbrückung:**

Lassen Sie die Kontrollkästchen für die Ports markiert, die Sie bei einer Verbindung zum Kabel-LAN sperren möchten. Deaktivieren Sie die Kontrollkästchen für die Ports, die Sie zulassen möchten.

### 3.3.5 Schritt 5: Gerätekontrolle definieren

Im Fenster *Port Control* können Sie für USB-, FireWire- und PCMCIA-Ports angeben, dass der Zugriff auf diese Porttypen eingeschränkt ist (dies gilt auch für WiFi-Ports, wie in *Schritt 8: WiFi-Kontrolle definieren* beschrieben). Durch die Auswahl von **Einschränken** können Sie im Fenster **Gerätekontrolle** detailliertere Angaben darüber machen, welche Geräte für den Zugriff auf diese Ports berechtigt sind.

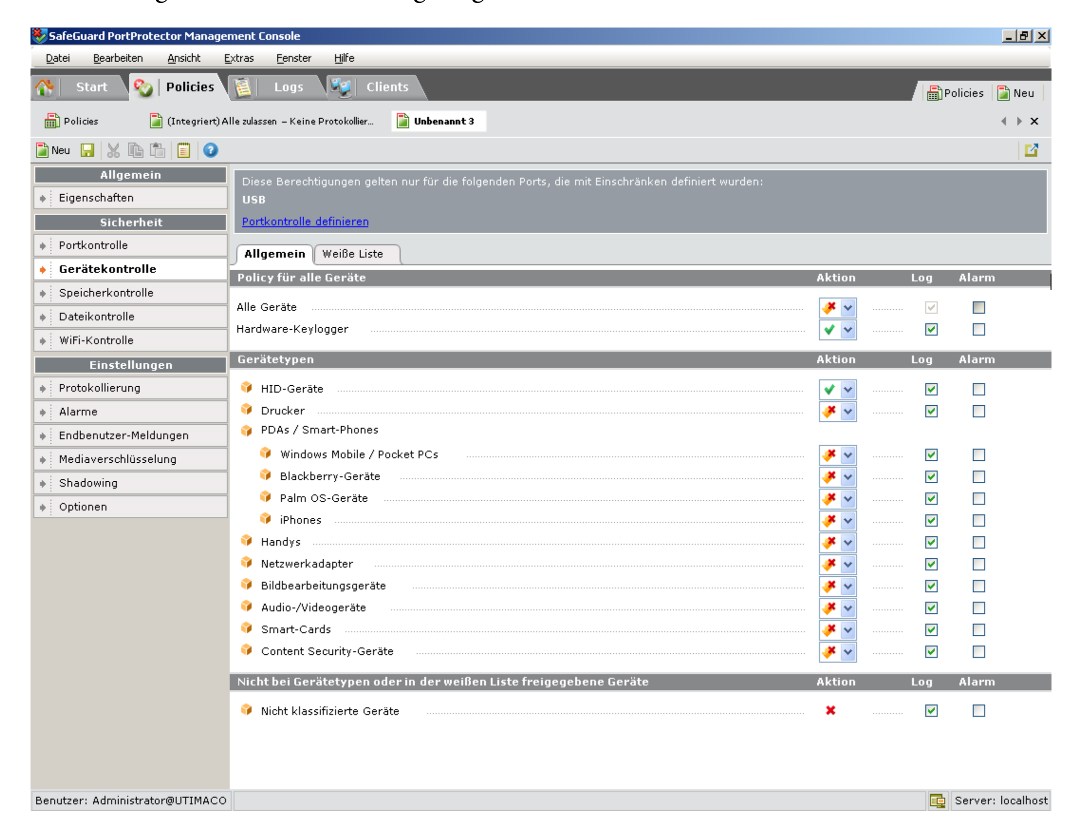
**So öffnen Sie das Fenster Gerätekontrolle:**

1 Klicken Sie auf der linken Seite im Menü Sicherheit auf die Schaltfläche Gerätekontrolle

ODER

Klicken Sie im Fenster Port Control auf den Link Gerätekontrolle definieren rechts neben der Option USB, FireWire oder PCMCIA.

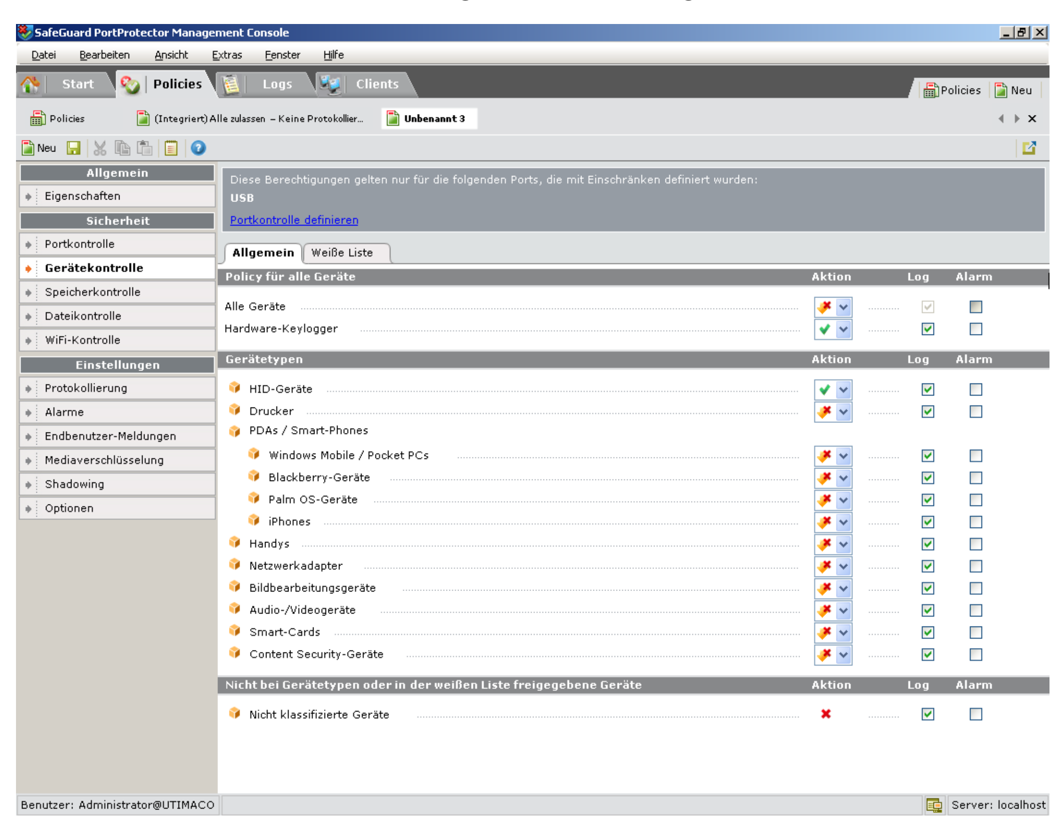
2 Das folgende Fenster wird angezeigt:




Das Fenster *Gerätekontrolle* enthält zwei Registerkarten: Die oben abgebildete Registerkarte *Allgemein*, auf der Sie angeben, welchen Gerätetypen der Zugriff erlaubt ist, und die Registerkarte *Weiße Liste*, auf der Sie angeben, welchen Gerätemodellen oder spezifischen Geräten der Zugriff erlaubt ist. Wenn ein Gerät auf keine der nachfolgend beschriebenen Arten zugelassen wird, ist es gesperrt. Der Aspekt der Gerätekontrolle gilt für **alle** eingeschränkten Ports.

Darüber hinaus können Sie mit *Gerätekontrolle* Optionen für Aktivitätslog und Alarm bis auf die Ebene der Gruppe spezifischer Geräte angeben. Das bedeutet: Sie können beispielsweise Aktivitäten bei Handys im Allgemeinen protokollieren, aber die Aktivitäten bei einer bestimmten Gruppe zugelassener Handys nicht.

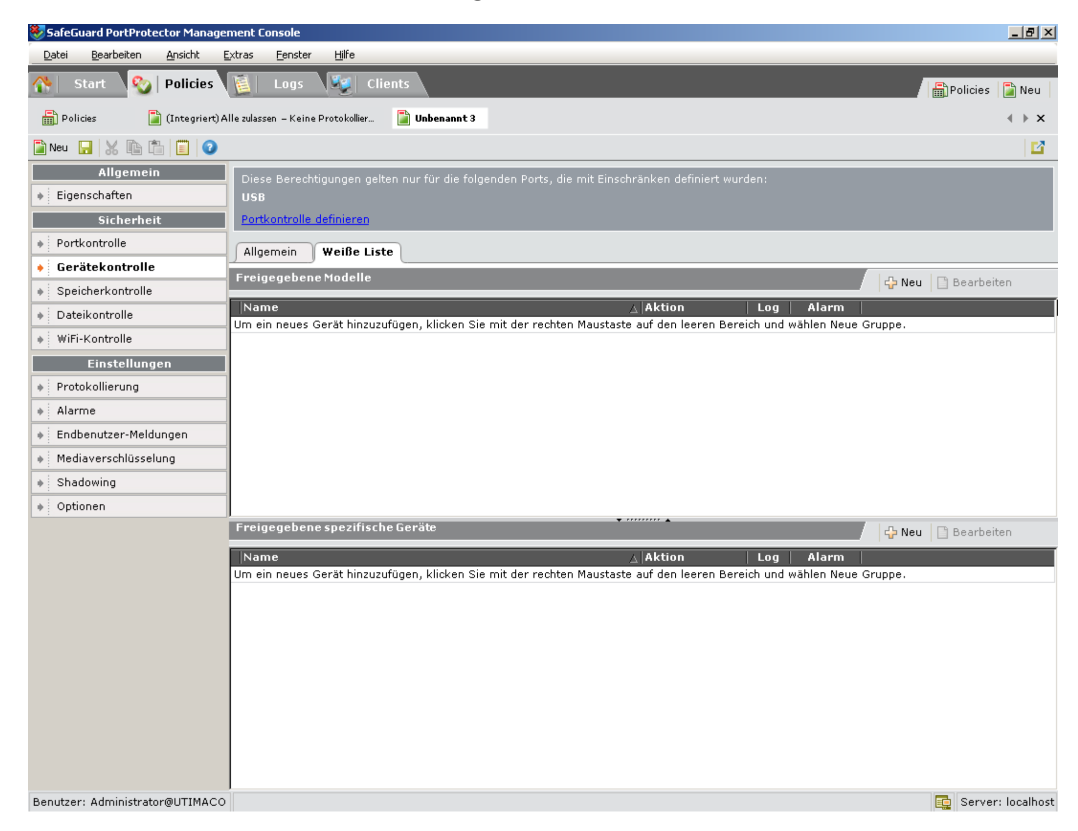
### 3.3.5.1 Gerätekontrolle – Registerkarte Allgemein




- **Policy für alle Geräte** (oberer Bereich): In diesem Bereich können Sie mit den Optionen **Zulassen**, **Einschränken** oder **Sperren** den Zugriff auf alle Gerätetypen zulassen, einschränken oder sperren. Wenn Sie **Zulassen** oder **Sperren** für **Alle Geräte** wählen, wird der Rest des Fensters deaktiviert.
  Hier legen Sie Log- und Alarmdefinitionen für die Geräteaktivität fest, wenn USB-, FireWire- oder PCMCIA-Ports zugelassen oder gesperrt sind.
  Sie können auch für Hardware-Keylogger die Optionen **Zulassen** oder **Sperren** wählen und Log- und Alarmeinstellungen definieren (Hardware-Keylogger sind in *Schutz vor Hardware-Keylogger* in *Kapitel 1, Einführung in SafeGuard PortProtector* erläutert).
- **Gerätetypen** (mittlerer Bereich): Wenn Sie die Option **Einschränken** für **Alle Geräte** wie im vorangegangenen Absatz beschrieben ausgewählt haben, können Sie mit dieser Option den Zugriff auf ein Gerät anhand seines Typs zulassen oder einschränken (z. B. Drucker, Netzwerkadapter oder Bildbearbeitungsgeräte). Die zur Auswahl stehenden Gerätetypen sind in SafeGuard PortProtector integriert. Wenn Sie ein Gerät zulassen möchten, das nicht hier aufgeführt ist, fügen Sie es Ihrer Liste der zugelassenen Geräte in der **Weiße Liste** hinzu. Verwenden Sie hierfür die unten beschriebene Option **Freigegebene Modelle** oder **Spezifische Geräte.** Eine Liste der unterstützten Gerätetypen finden Sie im Anhang unter Supported Device Types.
- **Nicht bei den Gerätetypen oder in der Weißen Liste freigegebene Geräte** (unterer Bereich): Wenn Sie die Option **Einschränken:** für **Alle Geräte** gewählt haben, können Sie mit dieser Option festlegen, ob eine versuchte Aktivität von Geräten unbekannten Typs (die gemäß Voreinstellung gesperrt sind) protokolliert und/oder dafür ein Alarm erzeugt werden soll. Weitere Informationen finden Sie in *Zulassen/Sperren nicht klassifizierter Geräte.*

Eine Beschreibung für die Definition der Optionen in diesem Fenster finden Sie in *Definieren der Gerätekontrolle.*

### 3.3.5.2 Gerätekontrolle – Registerkarte Weiße Liste




Oberhalb der Registerkarten werden in einer Meldung die Ports angezeigt, die Sie auf **Einschränken** gesetzt haben. Wenn Sie Porteinstellungen ändern möchten, nehmen Sie diese Änderungen im Fenster *Portkontrolle* vor (Sie können auf Portkontrolle definieren klicken, um zum Fenster *Portkontrolle* zu wechseln).

Das Fenster ist in zwei Bereiche unterteilt:

- **Freigegebene Modelle** (oberer Bereich): Diese Option bezieht sich auf das Modell eines bestimmten Gerätetyps, wie etwa ein bestimmtes Modell der HP-Drucker, z. B. LaserJet 4050N.
- **Freigegebene spezifische Geräte** (unterer Bereich): Diese Option bezieht sich auf spezifische Geräte mit einer eindeutigen Seriennummer, d. h. tatsächlich ein spezifisches Gerät. Zum Beispiel: Der persönliche Drucker des CEO kann für den Anschluss freigegeben sein, während andere Drucker es nicht sind.

Freigegebene Gerätegruppen fügen Sie in diesen beiden Bereichen hinzu.

Auf der rechten Seite der Registerkarte stehen drei Schaltflächen zur Verfügung:

- **Neue Gruppe** ( ): Mit dieser Schaltfläche fügen Sie eine neue Gerätegruppe hinzu.
- **Gruppe bearbeiten** ( ): Mit dieser Schaltfläche bearbeiten Sie eine Gerätegruppe.
- **Gruppe löschen** ( ): Mit dieser Schaltfläche löschen Sie eine Gerätegruppe.

**Hinweis:** Dieses Fenster ist deaktiviert, wenn Sie die Option **Zulassen** oder **Sperren** in **Policy für alle Geräte** auf der Registerkarte *Allgemein* gewählt haben. Siehe *Definieren der Gerätekontrolle.*

**Hinweis:** Falls ein Gerät zu mehreren Gruppen gehört, und diese Gruppen dieselben Berechtigungen haben, wird SafeGuard PortProtector die Gruppen willkürlich auswählen.

Wenn die Gruppen nicht dieselben Log- und Alarmeinstellungen haben, ist nicht vorhersehbar, welche Einstellungen angewendet werden.

Eine Beschreibung für die Definition der Optionen in diesem Fenster finden Sie in *Definieren der Gerätekontrolle.*

### 3.3.5.3 Definieren der Gerätekontrolle

**So definieren Sie die Gerätekontrolle:**

1 Klicken Sie im Fenster *Gerätekontrolle* auf die Registerkarte *Allgemein*, falls sie nicht die aktive Registerkarte ist.
Im oberen Teil des Fensters sind die Ports aufgelistet, die als **Eingeschränkt** im Fenster *Portkontrolle* definiert wurden, wie in *Schritt 4: Portkontrolle definieren beschrieben.* Die Geräte, die Sie – wie in diesem Abschnitt beschrieben – im Fenster *Gerätekontrolle* zulassen oder sperren, gelten nur für diese Ports.

2 Im Abschnitt *Policy für alle Geräte* geben Sie in der Dropdown-Liste *Aktion* mit **Zugelassen** ( ), **Eingeschränkt**( ) oder **Gesperrt** ( ) an, ob alle Geräte zugelassen, eingeschränkt oder gesperrt sind.

**Hinweis:** Wählen Sie **Zulassen** oder **Sperren**, wenn Sie zu diesem Zeitpunkt keine granulare Gerätekontrolle wünschen. Alternativ können Sie diese Option nutzen, wenn Sie bestehende Definitionen überschreiben, sie aber zu einem späteren Zeitpunkt wieder verwenden möchten.

3 Wenn Sie **Zulassen** oder **Sperren** für *Alle Geräte* wählen, können Sie außerdem angeben, ob Geräteaktivitäten protokolliert und/oder ob Alarme generiert werden sollen. Hierfür markieren Sie die Kontrollkästchen **Log** bzw. **Alarm**.
Wenn Sie **Zulassen** oder **Sperren** für *Alle Geräte* **wählen,** brauchen Sie im Fenster *Gerätekontrolle* nichts weiter zu tun; Sie fahren dann fort mit *Schritt* 6: Speicherkontrolle definieren.
Wenn Sie **Einschränken** für *Alle Geräte* wählen, legen Sie die Log- und Alarmdefinitionen für die verschiedenen Gerätetypen im Abschnitt *Gerätetypen* wie nachfolgend beschrieben fest.

4 Wenn Sie **Einschränken** für *Alle Gerätes* gewählt haben, geben Sie an, ob Hardware-Keylogger (*in Schutz vor Hardware Keylogger in Kapitel 1, Einführung in SafeGuard PortProtector*, erläutert) **Zugelassen** oder **Gesperrt** sind. Sie können zudem definieren, ob die Identifizierung und/oder Sperrung eines Hardware-Keyloggers protokolliert und/oder ob ein Alarm generiert werden soll.

**Hinweis:** Wenn der SafeGuard PortProtector Client vermutet, dass ein USB Hardware-Keylogger an die Tastatur angeschlossen ist und Hardware-Keylogger auf **Gesperrt** gesetzt sind, ist auch die Tastatur gesperrt. Empfehlen Sie dem Benutzer, die Tastatur direkt an den Computer anzuschließen, um sie zu aktivieren. Darüber hinaus können Sie den Speicher des SafeGuard PortProtector Client zurücksetzen, so dass die Tastatur wieder wie gewohnt funktioniert (siehe hierzu in *Zurücksetzen von Tastaturen (Tastatur-Hubs freigeben)* in *Kapitel 9, Endbenutzer-Erfahrung*).

**Hinweis:** Wenn Sie Hardware-Keylogger sperren, werden sowohl USB als auch PS/2 Key Logger gesperrt. Wenn SafeGuard PortProtector Client gegen PS/2 Key Logger schützt, wird keine Benutzermeldung angezeigt. Der Key Logger wird dennoch unbrauchbar, da die von ihm protokollierten Informationen zerstückelt werden.

Beachten Sie darüber hinaus Folgendes: Wenn ein PS/2 Key Logger blockiert wird und mit einer PS/2 Keyboard Video Mouse (KVM) gearbeitet wird, kann nicht mehr über die Tastatur zwischen Computern umgeschaltet werden. In diesem Fall müssen Sie die KVM betätigen.

5 Wenn Sie **Einschränken** für *Alle Geräte* wählen, legen Sie die Berechtigungen für jeden **Gerätetyp** in der Dropdown-Liste *Aktion* wie folgt fest:

- **Zulassen ( ):** Lässt alle Geräte dieses Typs zu.
- **Einschränken ( ):** Alle Geräte sind gesperrt, es sei denn sie sind auf der Registerkarte *Ausnahmen* speziell freigegeben, siehe auch *Freigeben von Geräten und WiFi-Verbindungen*.

6 Markieren Sie das Kontrollkästchen **Log**, wenn Geräteaktivitäten protokolliert werden sollen. Wenn dieses Kästchen markiert ist, wird ein Ereignis protokolliert, sobald ein Gerät dieses Typs angeschlossen wird. Das wird dann in der Logs-Welt angezeigt.

7 Markieren Sie das Kontrollkästchen **Alarm**, wenn Geräteaktivitäten einen Alarm auslösen sollen. Auch die Alarme werden in der Logs-Welt angezeigt.

8 Definieren Sie die Optionen **Log** bzw. **Alarm** für *Nicht klassifizierte Geräte* unten im Fenster im Bereich **Nicht bei den Gerätetypen oder in der Weißen Liste freigegebene Geräte**. Das Feld **Aktion** kann in diesem Fenster nicht bearbeitet werden. Der Zugriff auf nicht klassifizierte Geräte wird auf der Registerkarte *Policies* im Fenster *Administration* definiert, siehe auch *Zulassen/Sperren nicht klassifizierter Geräte*. Durch diese Einstellungen wird festgelegt, ob hier **Gesperrt** ( ) oder **Zugelassen** ( ) angezeigt wird.

9 Wählen Sie bei **Freigegebene Modelle** die freigegebenen Modelle und bei **Spezifische Gerätes** die spezifischen Geräte aus, die den zugelassenen Geräten auf der Registerkarte *Weiße Liste* hinzugefügt werden sollen, siehe auch *Freigeben von Geräten und WiFi-Verbindungen*.

## 3.3.6 Schritt 6: Speicherkontrolle definieren

Speichergeräte sind normalerweise die Hauptträger für das Durchsickern von Informationen in einer Organisation. Deshalb sind standardmäßig alle Speichereinheiten gesperrt, es sei denn, Sie geben etwas anderes an.

Mit SafeGuard PortProtector können Sie den Zugriff steuern und kontrollieren, indem Sie vollen Zugang zulassen, sperren oder nur schreibgeschützten Zugang für Geräte zulassen, die als Speichergeräte identifiziert wurden. Dazu zählen Wechselmedien wie Disk-on-Keys, Digitalkameras etc. sowie herkömmliche Geräte wie Diskettenlaufwerke, CD/ DVD-Laufwerke, externe Festplatten und Bandlaufwerke. Für Wechselspeichergeräte können Sie den Zugang auch auf organisatorisch verschlüsselte Geräte beschränken (siehe *SafeGuard PortProtector* Speicherverschlüsselung im Kapitel *Einführung in SafeGuard PortProtector*.

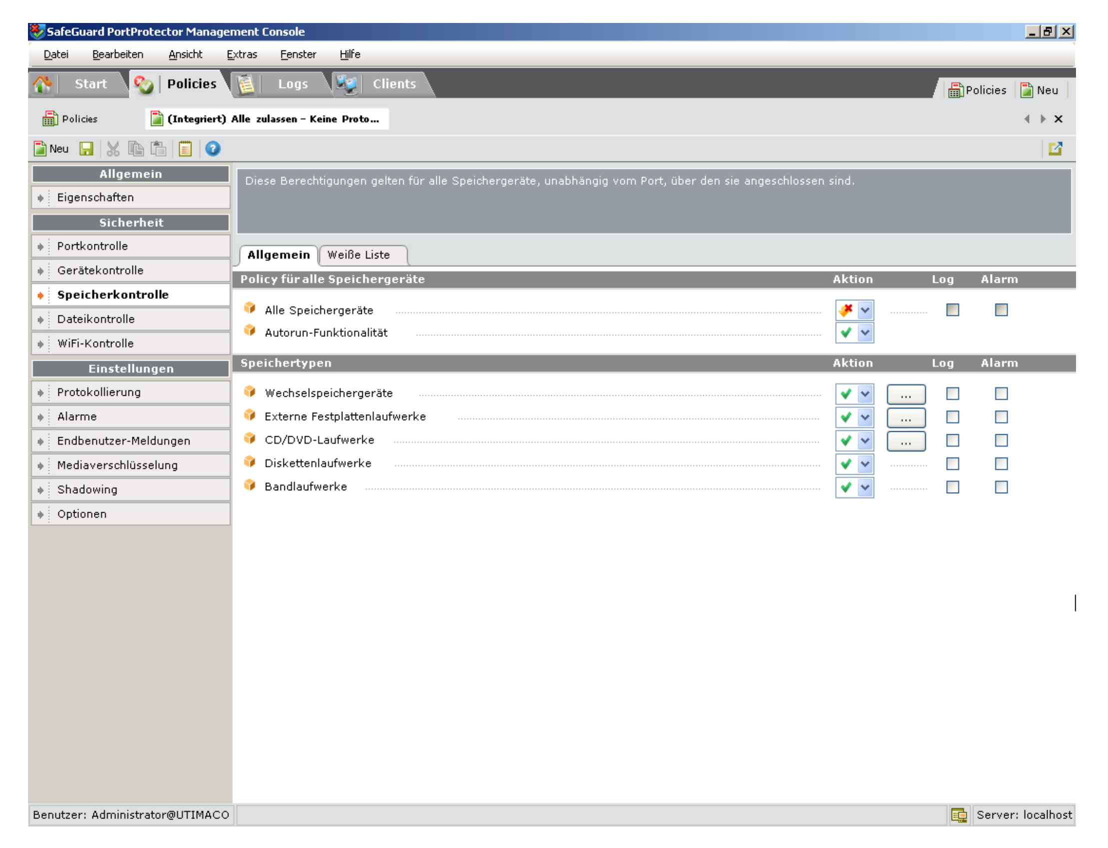
**Hinweis:** Die Schreibschutz-Option **Schreibgeschützt** ist für Bandlaufwerke nicht verfügbar.

Der Aspekt der Speicherkontrolle wird auf allen Ports durchgesetzt, an denen ein Speichergerät angeschlossen werden kann. Dazu zählen Ports, die auf **Zugelassen** oder **Eingeschränkt** gesetzt sind, sowie Ports, die nicht durch SafeGuard PortProtector geschützt sind. An einem auf **Gesperrt** gesetzten Port sind alle Speichergeräte gesperrt, weil die Sperrung so wirkt, als wären die Kabel abgetrennt.

### 3.3.6.1 Anzeigen des Fensters Speicherkontrolle

**So öffnen Sie das Fenster *Speicherkontrolle*:**

Klicken Sie auf der linken Seite im Menü *Sicherheit* auf die Schaltfläche **Speicherkontrolle**. Das folgende Fenster wird angezeigt:




Das Fenster*Speicherkontrolle* enthält zwei Registerkarten: Die Registerkarte *Allgemein*, auf der Sie angeben, welchen Speichertypen der Zugriff auf die internen Plattenverschlüsselungseinstellungen erlaubt ist, und die Registerkarte *Weiße Liste*, auf der Sie angeben, welchen Gerätemodellen oder spezifischen Geräten der Zugriff erlaubt ist.

### 3.3.6.2 Speicherkontrolle – Registerkarte General

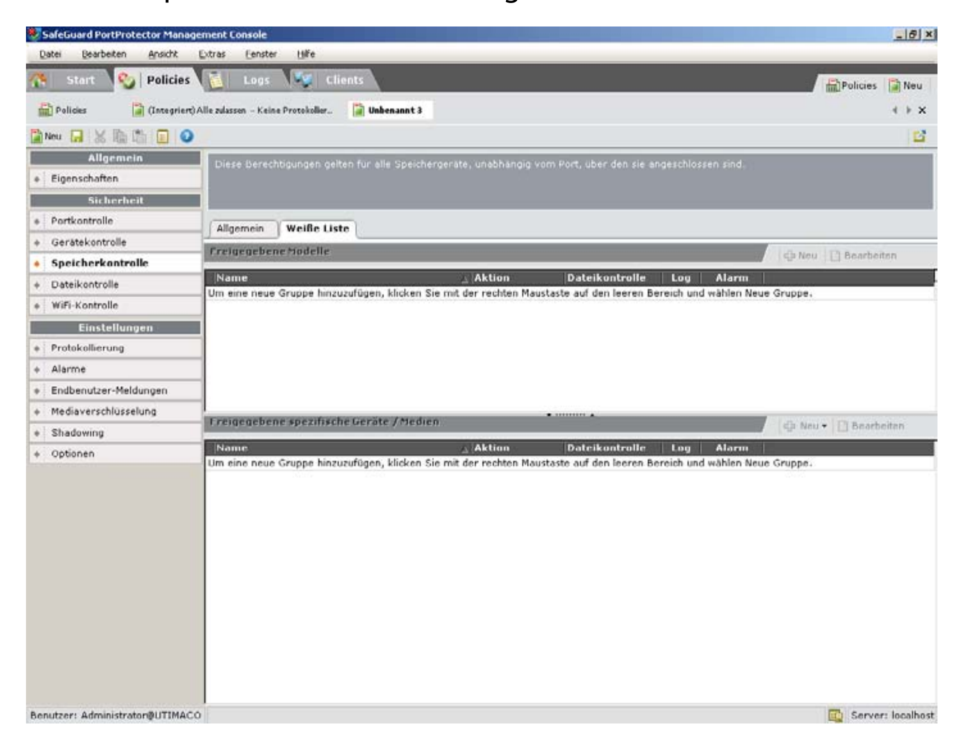
Dieses Fenster enthält folgende Bereiche:

- **Policy für alle Speichergeräte** (oberer Bereich): In diesem Bereich können Sie mit den Optionen **Zulassen**, **Einschränken** oder **Sperren** den Zugriff auf alle Speichergeräte zulassen, einschränken oder sperren. Wenn Sie **Zulassen** oder **Sperren** für **Alle Speichergeräte** wählen, wird der Rest des Fensters deaktiviert.
  Hier legen Sie Log- und Alarmdefinitionen für die Aktivität der Speichergeräte fest, wenn USB-, FireWire- oder PCMCIA-Ports zugelassen oder gesperrt sind.
  Sie können auch festlegen, ob Sie die Autorun-Funktion, die bei manchen Speichergeräten wie etwa CD/DVD vorhanden ist, zulassen oder sperren möchten (siehe auch *U3 Smartdrive und Autorun-Kontrolle* in *Kapitel 1, Einführung in SafeGuard PortProtector*).
- **Speichertypen** (mittlerer Bereich): Wenn Sie die Option **Einschränken** für *Alle Speichergeräte* wie im vorangegangenen Absatz beschrieben ausgewählt haben, können Sie mit dieser Option den Zugriff auf ein Speichergerät anhand seines Typs zulassen oder einschränken (z. B. Wechselmedien oder CD/DVD-Laufwerke). Die zur Auswahl stehenden Gerätetypen sind in SafeGuard PortProtector integriert. Hierzu gehören:
  - **Wechselmedien:** Gilt für alle Plug-and-Play-Speichergeräte, wie etwa Disk-on-Keys, Digitalkamera, portable MP3-Player etc.
  - **Externe Festplatten**
  - **CD/DVD-Laufwerke**
  - **Diskettenlaufwerke**
  - **Bandlaufwerke**

Mit Hilfe der *Weißen Liste* können Sie mit den Optionen **Freigegebenes Modell** oder **Spezifische Geräte** zugelassene Modelle bzw. spezifische Geräte hinzufügen. Eine Beschreibung der unterstützten Gerätetypen finden Sie im Anhang unter *Supported Device Types*.

Eine Beschreibung für die Definition der Optionen in diesem Fenster finden Sie in *Definieren der Speicherkontrolle.*

### 3.3.6.3 Speicherkontrolle – Registerkarte Weiße Liste




Das Fenster ist in zwei Bereiche unterteilt:

- **Freigegebene Modelle** (oberer Bereich): Diese Option bezieht sich auf die Modelle eines bestimmten Speichergerätetyps, wie etwa ein bestimmtes Disk-on-Key-Modell.
- **Freigegebene spezifische Geräte/Medien** (unterer Bereich): Diese Option bezieht sich auf zwei Arten von Gruppen:
  - Spezifische Geräte mit einer eindeutigen Seriennummer, d. h. tatsächlich ein spezifisches Gerät. So kann z. B. das persönliche Disk-on-Key-Gerät des CEO für den Anschluss freigegeben sein, während andere Disk-on-Key-Geräte es nicht sind.
  - Freigegebene CD/DVD-Medien, die zuvor gescannt und mit einem "Fingerprint" versehen wurden.

In diesen beiden Bereichen fügen Sie freigegebene Speichergerätegruppen hinzu.

In jeder Gruppe Sie können Folgendes definieren:

- Aktion (Zulassen/Verschlüsseln/Schreibgeschützt) – für Mediengruppen nicht relevant
- Berechtigungen (Disk-on-Key Smart-Funktionalität oder Dateikontrolle) – für Mediengruppen nicht relevant
- Logeinstellungen
- Alarmeinstellungen

Auf der rechten Seite der Registerkarte stehen drei Schaltflächen zur Verfügung:

- **Neue Gruppe** (): hiermit fügen Sie eine neue Gerätegruppe hinzu.
- **Gruppe bearbeiten** (): hiermit bearbeiten Sie eine Gerätegruppe.
- **Gruppe löschen** (): hiermit löschen Sie eine Gerätegruppe.

**Hinweis:** Dieses Fenster ist deaktiviert, wenn Sie die Option **Zulassen** oder **Sperren** in Policy für alle Speichergeräte auf der Registerkarte *Allgemein* gewählt haben.

Eine Beschreibung für die Definition der Einstellungen in diesem Fenster finden Sie in *Definieren der Speicherkontrolle.*

### 3.3.6.4 Definieren der Speicherkontrolle

**So definieren Sie die Speicherkontrolle:**

1 Klicken Sie im Fenster *Speicherkontrolle* auf die Registerkarte *General*, sofern sie nicht aktiv ist.

2 Im Abschnitt *Policy für alle Speichergeräte* geben Sie für **Alle Speichergerätes** mit **Zulassen/Zugelassen** (✔), **Einschränken/Eingeschränkt** () oder **Sperren/Gesperrt** (✖) an, ob alle Speichergeräte zugelassen, eingeschränkt oder gesperrt sind, indem Sie die entsprechende Option in der Dropdown-Liste *Aktion* auswählen.

   **Hinweis:** Wählen Sie **Zulassen** oder **Sperren**, wenn Sie zu diesem Zeitpunkt keine granulare Speichergerätekontrolle wünschen. Alternativ können Sie diese Option nutzen, wenn Sie bestehende Definitionen überschreiben, sie aber zu einem späteren Zeitpunkt wieder verwenden möchten.

3 Wenn Sie **Zulassen** oder **Sperren** für **Alle Speichergeräte** wählen, können Sie auch angeben, ob Geräteaktivitäten protokolliert und/oder ob Alarme generiert werden sollen. Hierfür markieren Sie die Kontrollkästchen **Log** bzw. **Alarm**.

4 Wenn Sie **Zulassen** oder **Sperren** für **Alle Speichergeräte** wählen, brauchen Sie im Fenster *Speicherkontrolle* nichts weiter zu tun; Sie fahren dann fort mit *Schritt 8: WiFi-Kontrolle definieren*.
   Die übrigen Anleitungen in diesem Abschnitt sind nur von Bedeutung, wenn Sie **Einschränken** für **Alle Speichertypen** gewählt haben.

5 In der Dropdown-Liste *Aktion* können Sie die **Autorun-Funktionalität** mit **Zulassen** zulassen oder mit **Sperren** sperren (eine Erklärung dieser Funktionalität finden Sie in *U3 Smartdrive und Autorun-Kontrolle* in *Kapitel 1, Einführung in SafeGuard PortProtector).*

6 Legen Sie die Berechtigungen für **Speichertypen** in der Dropdown-Liste *Aktion* wie folgt fest:

- **Zulassen** (✔): Lässt alle Speichergeräte dieses Typs zu.
- **Verschlüsseln** (): Der Zugriff auf diesen Speichergerätetyp ist nur dann zugelassen, wenn er von der Organisation verschlüsselt wurde. Wenn ein unverschlüsseltes Gerät angeschlossen wird, wird der Endbenutzer aufgefordert, es zu verschlüsseln, siehe auch *Verschlüsselung und Entschlüsselung von Wechselspeichergeräten* in *Kapitel 9, Endbenutzer-Erfahrung*. Diese Art der Berechtigung ist für **Wechselspeichergeräte, externe Festplatten und für CD/DVD** verfügbar. Eine Erläuterung, wie Endbenutzer die Verschlüsselung durchführen können, finden Sie im Kapitel *Endbenutzer-Erfahrung*.

**Hinweis:** Wenn ein Gerät oder Medium an einer Stelle auf **Verschlüsseln** (wie etwa hier) und an einer anderen Stelle auf **Zulassen** (z. B. in der *Weißen Liste*) gesetzt ist, gilt im Rahmen der Regel "mit den meisten Berechtigungen" die Berechtigung **Zulassen**.

Wenn ein Gerät oder Medium an einer Stelle auf **Verschlüsseln** (wie etwa hier) und an einer anderen Stelle auf **Schreibgeschützt** (z. B. in den *Ausnahmen*) gesetzt ist, gilt die Berechtigung **Verschlüsseln**.

- **Schreibgeschützt** ( ): Lässt nur das Lesen von den Speichergeräten dieses Typs über ungesperrte Ports zu. Bei CDs und DVDs bedeutet die Einstellung **Schreibgeschützt**, dass sie nicht zum Brennen benutzt werden können.

Gemäß der Regel "mit den meisten Berechtigungen" gilt: Wenn ein Gerät oder Medium an einer Stelle auf **Schreibgeschützt** (wie etwa hier) und an einer anderen Stelle auf **Zulassen** (z. B. in den *Ausnahmen*) gesetzt ist, gilt die Berechtigung **Zulassen**.

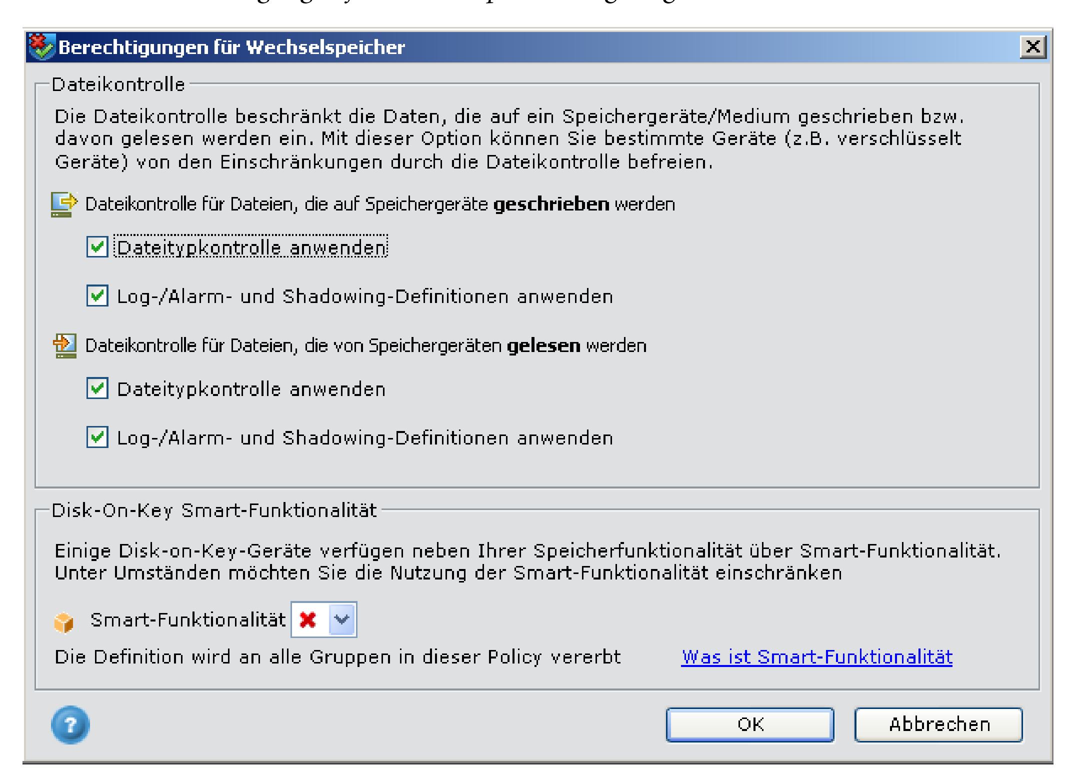
7 Verschlüsselung interner Festplatten (unterer Bereich): Wählen Sie Nicht konfiguriert, Entschlüsseln oder Verschlüsseln. Wenn Sie Nicht konfiguriert wählen, ist keine Verschlüsselungspolicy (Verschlüsseln oder Entschlüsseln) festgelegt. Wenn Sie eine mit einem bereits verschlüsselten Computer verknüpfte Policy auf Entschlüsseln ändern, werden die Informationen auf dem Computer entschlüsselt. Wenn Sie Verschlüsseln wählen, startet die Verschlüsselung der internen Festplatte(n) beim nächsten Anmelden des Benutzers am Computer. Diese Einstellungen gelten nur für Computer und nicht für die mit dieser Policy verknüpften Benutzer.

#### 3.3.6.4.1 Weitere Berechtigungen

Für Wechselspeichergeräte, externe Festplatten und CD/DVD können Sie weitere Berechtigungen festlegen.

**So legen Sie weitere Berechtigungen für Wechselspeichergeräte fest:**

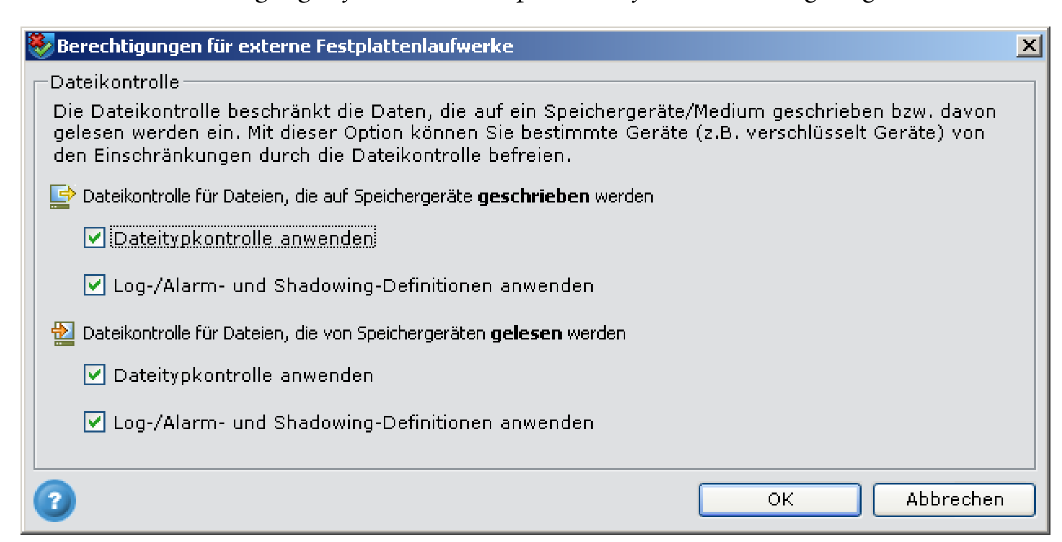
Klicken Sie auf die Schaltfläche **Weitere Berechtigungen** [...] für Wechselspeichergeräte. Das Fenster *Berechtigungen für Wechselspeicher* angezeigt:




Anleitungen zur Vergabe von Berechtigungen finden Sie in Festlegen der *Berechtigungen für Wechselspeicher*.

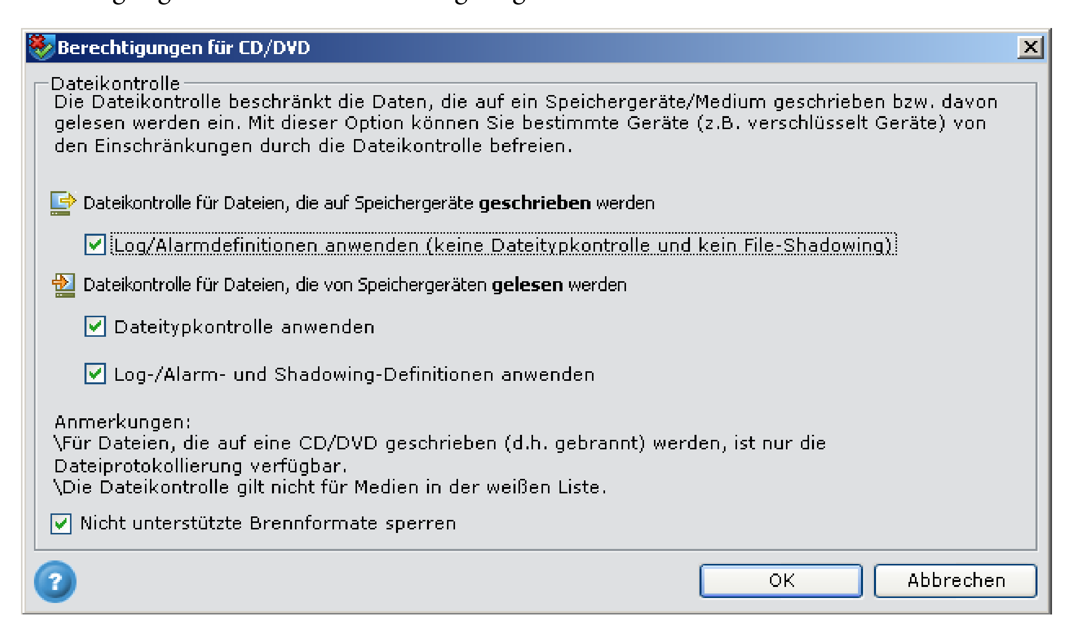
**So legen Sie weitere Berechtigungen für externe Festplatten fest:**

Klicken Sie auf die Schaltfläche **Weitere Berechtigungen** für externe Festplatten. Das Fenster *Berechtigungen für externe Festplattenlaufwerke* wird angezeigt:




**So legen Sie weitere Berechtigungen für CD/DVD fest:**

Klicken Sie auf die Schaltfläche **Weitere Berechtigungen** für CD/DVD. Das Fenster Berechtigungen für *CD/DVD* wird angezeigt:




Anleitungen zur Vergabe von Berechtigungen finden Sie in *Festlegen der Berechtigungen* für CD/DVD.

#### 3.3.6.4.1.1 Festlegen der Berechtigungen für Wechselspeicher

Mit diesen Berechtigungen können Sie Wechselspeichergeräte von der Dateikontrolle befreien (siehe *Schritt 7: Dateikontrolle definieren* in *Kapitel 3, Definieren von Policies*) und nach die Nutzung der Smart-Funktionalität sperren (siehe nachstehende Erklärung).
Eventuell möchten Sie im Falle verschlüsselter Geräte Wechselspeichergeräte von der Dateikontrolle ausnehmen, wenn Sie z. B. wissen, dass diese Geräte geschützt sind. Dadurch wird verhindert, dass überflüssige Logs erzeugt werden und sicherer Inhalt überprüft werden muss.

Die Standarddefinitionen sind auf **Anwenden** *der Dateikontrolle für Dateien, die auf diese Speichergeräte geschrieben bzw. von ihnen gelesen werden* und **Zulassen** *der Smart-Funktionalität* gesetzt.

**So legen Sie die Berechtigungen für Wechselspeichergeräte fest:**

1 Geben Sie die erforderlichen Definitionen in diesem Fenster wie folgt an:

- **Dateikontrolle:** Deaktivieren Sie in diesem Abschnitt das entsprechende Kontrollkästchen (*Dateitypkontrolle anwenden*/*Log-/Alarm- und Shadowing-Definitionen anwenden*), um Dateien, die auf freigegebene Geräte geschrieben bzw. von freigegebenen Geräten gelesen werden, nach Bedarf von der Dateikontrolle auszunehmen (um sie wieder der Dateikontrolle zu unterwerfen, markieren Sie das entsprechende Kontrollkästchen wieder).
- **Disk On Key Smart Functionality:** Bestimmte Disk-On-Key-Geräte, wie beispielsweise U3-Geräte, bieten neben den grundlegenden Speicherfunktionen eine intelligente Funktionalität. Mit Hilfe dieser Funktionalität können diese Geräte Anwendungen speichern und ausführen, sobald sie an einen Hostcomputer angeschlossen sind. Möglicherweise möchten Sie diese Geräte auf ihre Speicherfunktion beschränken und die darauf befindlichen Anwendungen sperren. Hierzu wählen Sie Block ( ). Alle zu dieser Policy gehörenden Gerätegruppen {'erben' diese Definition, es sei denn, Sie überschreiben sie mit gruppenspezifischen Definitionen, siehe auch *Weitere Einstellungen für Gerätegruppen*.

2 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster *Berechtigungen für Wechselspeicher* zu schließen.

#### 3.3.6.4.1.2 Festlegen der Berechtigungen für externe Festplatte

Mit diesen Berechtigungen können Sie externe Festplatten von der Dateikontrolle befreien (siehe *Schritt 7: Dateikontrolle definieren* in *Kapitel 3, Definieren von Policies*).

Die Standarddefinitionen sind auf **Anwenden** *der Dateikontrolle für Dateien, die auf diese Speichergeräte geschrieben bzw. von ihnen gelesen werden* gesetzt.

**So legen Sie Berechtigungen für externe Festplatten fest:**

1 Deaktivieren Sie im Abschnitt *Dateikontrolle* das entsprechende Kontrollkästchen (*Dateitypkontrolle anwenden*/*Log-/Alarm- und Shadowing-Definitionen anwenden*), um Dateien, die auf freigegebene Geräte geschrieben bzw. von freigegebenen Geräten gelesen werden, nach Bedarf von der Dateikontrolle auszunehmen (um sie wieder der Dateikontrolle zu unterwerfen, markieren Sie das entsprechende Kontrollkästchen wieder).

2 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster *Berechtigungen für externe Festplatten* zu schließen.

#### 3.3.6.4.1.3 Festlegen der Berechtigungen für CD/DVD

Mit diesen Berechtigungen können Sie CD/DVDs von der Dateikontrolle befreien (siehe *Schritt 7: Dateikontrolle definieren* in *Kapitel 3, Definieren von Policies*).

Die Standarddefinitionen sind auf **Anwenden** *der Dateikontrolle für Dateien, die auf diese Speichergeräte geschrieben bzw. von ihnen gelesen werden* gesetzt.

**So legen Sie Berechtigungen für CD/DVD fest:**

1 Deaktivieren Sie im Abschnitt *Dateikontrolle* das entsprechende Kontrollkästchen (*Dateitypkontrolle anwenden/Log-/Alarm- und Shadowing-Definitionen anwenden*), um Dateien, die auf freigegebene Geräte geschrieben bzw. von freigegebenen Geräten gelesen werden, nach Bedarf von der Dateikontrolle auszunehmen (um sie wieder der Dateikontrolle zu unterwerfen, markieren Sie das entsprechende Kontrollkästchen wieder).

**Hinweis:** Die Dateikontrolle kann auf Dateien angewandt werden, die von CD/DVDs gelesen werden, aber nicht auf Dateien, die darauf geschrieben werden.

**Hinweis:** Die Dateikontrolle wird nicht auf Medien angewandt, die in der Ausnahmenliste stehen.

2 Beim Schreiben auf eine CD/DVD kann SafeGuard PortProtector Dateien protokollieren, die die folgenden drei Bedingungen erfüllen:

- Die Brennmethode ist 'Track At Once'
- Das Dateisystem basiert auf ISO (d. h. ISO, ISO+JOILET, ISO+UDF)
- Es ist die erste Schreib-Sitzung auf dieser CD.

Dateien, die nicht alle drei Bedingungen erfüllen, werden nicht protokolliert.

Das Schreiben von Dateien auf eine CD/DVD, die von SafeGuard PortProtector nicht protokolliert werden können, ist standardmäßig gesperrt. Dem Benutzer wird eine SafeGuard PortProtector Client-Meldung angezeigt, wenn er versucht, ein nicht unterstütztes Format zu schreiben.

Wenn Sie das Schreiben dieser Dateien zulassen möchten, deaktivieren Sie das Kontrollkästchen **Nicht unterstützte Brennformate sperren**.

3 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster *Berechtigungen für CD/DVD* zu schließen.

### 3.3.7 Schritt 7: Dateikontrolle definieren

Mit SafeGuard PortProtector können Sie nicht nur Berechtigungen für Speichergeräte festlegen, sondern auch für die Dateien, die zu/von diesen Geräten übertragen werden. Hierfür werden die Dateien beim Transfer zu/von externen Speichergeräten auf ihren Typ hin überprüft. Diese Technologie ermöglicht eine äußerst zuverlässige Klassifizierung der Dateien, bei der die Inhalte des Datei-Headers anstelle der Dateierweiterung geprüft werden. So wird verhindert, dass Benutzer den Schutz einfach durch Ändern der Dateierweiterung umgehen können. Dank nahezu 200 integrierter Dateitypen aller gängigen Anwendungen, die in 14 Dateikategorien eingeordnet sind, können Policies so detailliert definiert werden wie nie zuvor.

Da sowohl die auf externe Speichergeräte heruntergeladenen als auch auf den geschützten Endpunkt hochgeladenen Dateien geprüft werden, lassen sich mehrere Vorteile erzielen:

- Eine zusätzliche Schutzschicht, um das Durchsickern von Daten zu verhindern
- Verhinderung, dass Viren/Schadprogramme über externe Speichergeräte eingeschleppt werden
- Verhinderung, dass unsachgemäßer Inhalt über externe Speichergeräte eingebracht wird, wie etwa nicht lizenzierte Software, nicht lizenzierter Inhalt (z. B. Musik und Filme), nicht arbeitsbezogener Inhalt (z. B. persönliche Bilder) etc.

Mit dieser Funktion können Sie Policies definieren, die bestimmte Dateitypen auf den Eingangs- und Ausgangskanälen sperren. Hierzu gehören getrennte Definitionen für Eingangs- und Ausgangskanäle und die Unterstützung von weißen und schwarzen Listen.

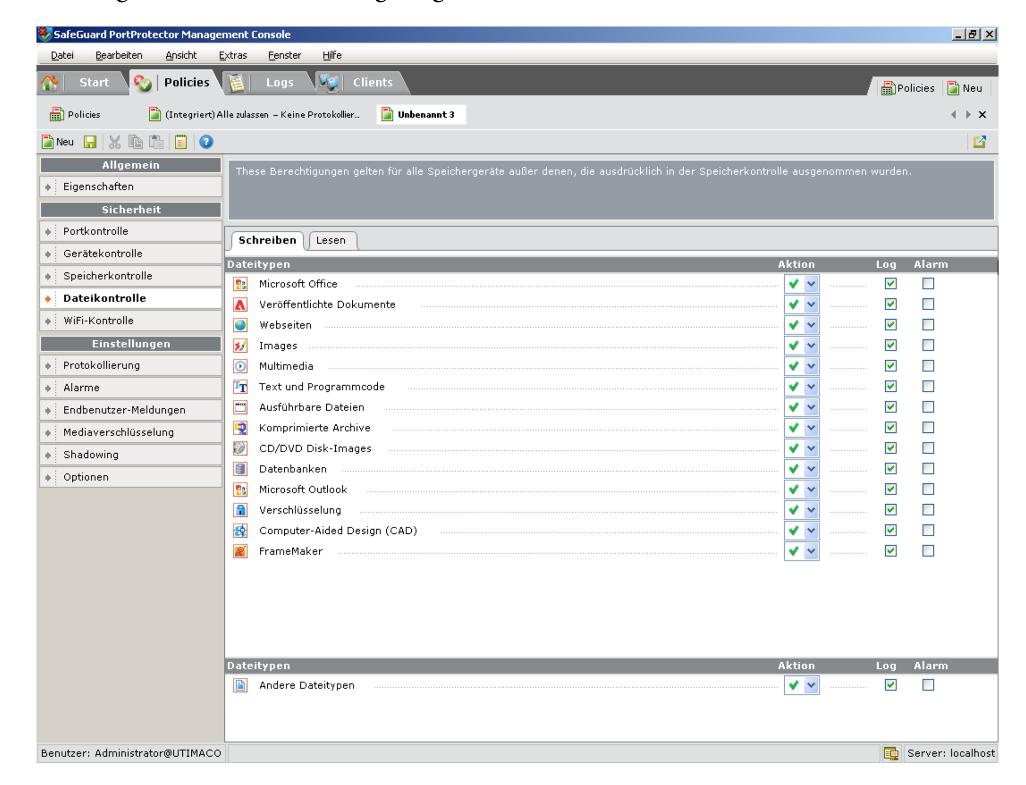
Die Dateikontrolle von SafeGuard PortProtector umfasst Folgendes:

- **Dateitypkontrolle –** die Möglichkeit, die Übertragung von Dateien anhand ihres Typs zu kontrollieren
- **Dateiprotokollierung –** die Möglichkeit, Logs bzw. Alarme beim Transfer bestimmter Dateitypen auszugeben (dies ersetzt die Dateiprotokollierungsfunktion früherer Versionen)
- **Inhaltsprüfung –** die Möglichkeit, den tatsächlichen Inhalt von Dateien eines angegebenen Typs zu überprüfen, bevor sie auf ein externes Speichergerät geschrieben werden, und zu bestimmen, ob der Inhalt sensibel ist.
- **Datei-Shadowing –** die Möglichkeit der Rückverfolgung und Erfassung von Kopien von Dateien, die zu/von externen Speichergeräten verschoben wurden (siehe *Einstellungen für Datei-Shadowing definieren).*

Die Dateikontrolle ist auf alle Wechselspeichergeräte, externe Festplatten und CD/DVD anwendbar.

**So öffnen Sie das Fenster *Dateikontrolle*:**

1 Klicken Sie auf der linken Seite im Menü *Sicherheit* auf die Schaltfläche **Dateikontrolle.** Das folgende Fenster wird angezeigt:




Das Fenster *Dateikontrolle* enthält zwei Registerkarten: Die Registerkarte *Schreiben*, auf der Sie die Berechtigungen für auf Speichergeräte geschriebene Dateitypen festlegen, und die Registerkarte *Lesen*, auf der Sie die Berechtigungen für von Speichergeräten gelesene Dateitypen festlegen. In diesem Fenster geben Sie auch für jeden Dateityp an, ob Sie eine Protokollierung oder Alarmauslösung für die Dateien des jeweiligen Typs wünschen. Eine Liste der unterstützten Dateitypen finden Sie im Anhang unter *Supported File Types*.

### 3.3.7.1 Dateikontrolle – Registerkarte Schreiben

Der obere T eil dieses Fensters enthält eine Liste der unterstützten Dateitypen. Für jeden Dateityp können Sie über das Menü *Aktion* Schreib-Berechtigungen festlegen. Mit den Kontrollkästchen können Sie Log- and Alarmeinstellungen auswählen.

Im unteren Teil des Fensters können Sie Berechtigungen sowie Log- und Alarmeinstellungen für andere Dateiformate festlegen, die nicht unter den unterstützten Dateitypen aufgeführt sind.

Eine Beschreibung für die Definition der Einstellungen in diesem Fenster finden Sie in *Definieren der Dateikontrolle*.

### 3.3.7.2 Dateikontrolle – Registerkarte Lesen

Der obere T eil dieses Fensters enthält eine Liste der unterstützten Dateitypen. Für jeden Dateityp können Sie über das Menü *Aktion* Lese-Berechtigungen festlegen. Mit den Kontrollkästchen können Sie Log- and Alarmeinstellungen auswählen.

Im unteren Teil des Fensters können Sie Berechtigungen sowie Log- und Alarmeinstellungen für andere Dateiformate festlegen, die nicht unter den unterstützten Dateitypen aufgeführt sind.

Eine Beschreibung für die Definition der Einstellungen in diesem Fenster finden Sie in *Definieren der Dateikontrolle*.

### 3.3.7.3 Definieren der Dateikontrolle

Hinweis: Die Dateikontrolle bezieht sich auf Dateien, die auf die folgenden externen Speichergeräte geschrieben bzw. von ihnen gelesen werden: Wechselspeichergeräte, externe Festplatten und CD/DVD-Laufwerke (bei CD/DVD kann die Dateikontrolle auf Dateien angewandt werden, die davon gelesen werden, aber nicht auf Dateien, die darauf geschrieben werden).

Sie können bei Bedarf eins oder mehrere dieser Speichergeräte von der Dateikontrolle ausnehmen. Eine Erklärung hierzu finden Sie in *Festlegen der Berechtigungen für* Wechselspeicher, *Festlegen der Berechtigungen für externe* Festplatte und *Festlegen der Berechtigungen für CD/DVD*.

**So definieren Sie die Dateikontrolle:**

1 Klicken Sie im Fenster *Dateikontrolle* auf die Registerkarte *Schreiben*.

2 Wählen Sie für jeden Dateityp die gewünschte Berechtigung im Menü *Aktion* wie folgt:

- **Zulassen ( ):** Lässt das Schreiben dieses Dateityps ohne Einschränkung zu.
- **Zulassen & kopieren ( ):** Lässt das Schreiben dieses Dateityps zu, wobei eine Kopie von jeder Datei angelegt wird, die von/zu externen Speichergeräten verschoben wird.

**Hinweis:** Nutzen Sie diese Option mit Bedacht, da hierdurch sowohl die Netzauslastung als auch Speicherressourcen beeinträchtigt werden können. Vorzugsweise sollten Sie sie anfangs in kleinen, gut definierten Bereichen Ihrer Organisation einsetzen.

- **Prüfen ( ):** Lässt das Schreiben dieses Dateityps zu, prüft aber vor dem Schreiben ihren Inhalt, um festzustellen, ob sie sensibel sind.

**Hinweis:** Die Option **Prüfen** erscheint nur dann im Menü *Aktion*, wenn die Funktion der Inhaltsprüfung aktiviert ist. In diesem Fall stehen die Aktionen Zulassen & Shadow nicht zur Verfügung.

- **Sperren ( ):** Sperrt das Schreiben dieses Dateityps.

3 Markieren Sie das Kontrollkästchen **Log** für die einzelnen Dateitypen, wenn Schreibaktivitäten protokolliert werden sollen. Wenn **Log** markiert ist, werden Logs für jede Datei erzeugt, die dann File Logs in der Logs-Welt eingesehen werden können (siehe *Kapitel 5, Anzeigen von Logs*). Eine Liste und Erklärung für die Felder der Dateilog-Datensätze finden Sie in *Struktur des Datei-Logs* in *Kapitel 5, Anzeigen von Logs*.

**Hinweis:** Wenn SafeGuard PortProtector den Transfer einer Datei von bzw. zu einem bestimmten Gerät einmal protokolliert hat, wird dies nicht noch einmal protokolliert, es sei denn, eine der folgenden Bedingungen wird erfüllt:

- Seit der letzten Protokollierung ist eine Stunde vergangen
- Der Computer wurde neu gestartet
- Das Gerät wurde neu angeschlossen.

Auf diese Weise wird verhindert, dass mehrere Logdatensätze geschrieben werden, wenn dieselbe Datei wiederholt auf dasselbe Gerät geschrieben wird (wenn z. B. ein Endbenutzer eine Datei auf einem Speichergerät bearbeitet und sie wiederholt speichert).

4 Markieren Sie das Kontrollkästchen **Alarm** für die einzelnen Dateitypen, wenn Schreibaktivitäten einen Alarm auslösen sollen.

5 Wiederholen die oben beschriebenen Schritte für jeden Dateityp und für die anderen Dateitypen, die unter Andere Dateitypen im unteren Teil des Fensters erscheinen.

**Hinweis:** Die Berechtigungen, die Sie bei Andere Dateitypen festlegen, gelten für jeden Dateityp, der nicht in der Liste im oberen Teil des Fensters steht.

**Hinweis:** Die Standardberechtigungen für alle Dateitypen sind **Zulassen** und **Log** (kein Alarm).

6 Klicken Sie auf die Registerkarte *Lesen*.

7 Führen Sie die oben beschriebenen Schritte 2-5 aus. Der einzige Unterschied zwischen den Registerkarten *Lesen* und *Schreiben* besteht darin, dass auf der Registerkarte *Lesen* die Option **Prüfen** nicht im Menü *Aktion* erscheint, weil nur ausgehende Dateien geprüft werden.

**Hinweis:** Die Standardberechtigungen für alle Dateitypen sind **Zulassen** (keine Logs oder Alarme).

**Hinweis:** Die Protokollierung von Dateien, die von Geräten gelesen werden, kann beispielsweise beim Installieren von Software zu einer übermäßigen Anzahl an Logdatensätze führen.

### 3.3.8 Schritt 8: WiFi-Kontrolle definieren

Zusätzlich zu Geräten kontrolliert und überwacht SafeGuard PortProtector Ihre WiFi-Verbindungen um sicherzustellen, dass die Clients nur autorisierte, sichere Verbindungen nutzen. Im Fenster *Port Control* können Sie mit **Eingeschränkt** festlegen, dass der Zugriff auf einen Port beschränkt ist. Durch die Auswahl von **Eingeschränkt** können Sie im Fenster **WiFi-Kontrolle** detailliertere Angaben darüber machen, welche Netze auf diesen Port zugreifen dürfen.

**Hinweis:** Wird die WiFi-Nutzung für einen Port eingeschränkt, überwacht und steuert SafeGuard PortProtector die WiFi-Verbindungen über die Microsoft WZC-Infrastruktur. Jeder Gerätetreiber, der ohne WZC einen Zugriff auf die Netzwerkkarte versucht, wird gesperrt. Außerdem ist WZC unter Windows 2000 nicht verfügbar.

Wenn Sie viele WiFi-Karten nutzen, die eigene Treiber verwenden, oder in Ihrer Organisation nur Windows 2000 einsetzen, können Sie WiFi als Port nur auf **Zulassen** oder **Sperren** setzen.

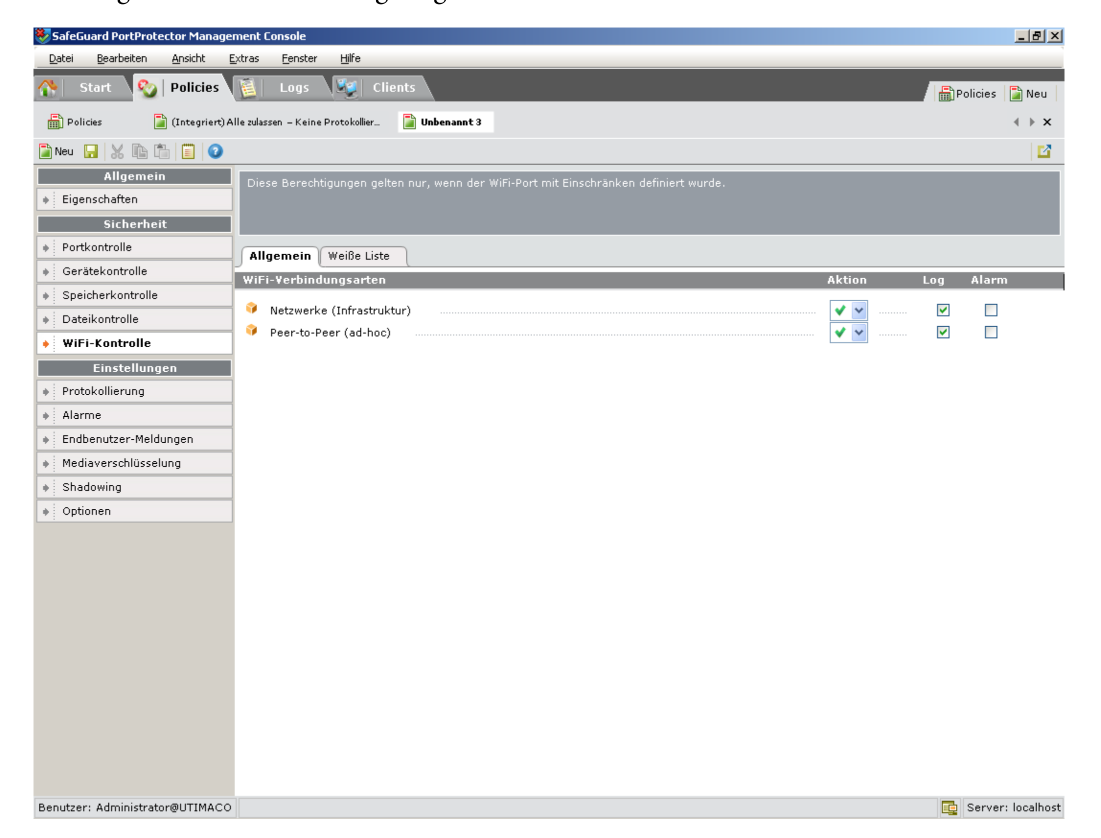
**So öffnen Sie das Fenster *WiFi-Kontrolle*:**

Klicken Sie auf der linken Seite im Menü *Sicherheit* auf die Schaltfläche **WiFi-Kontrolle**

ODER

Klicken Sie im Fenster *Portkontrolle Control* auf den Link **WiFi-Kontrolle definieren** rechts neben der Option WiFi.

Das folgende Fenster wird angezeigt:




Das Fenster *WiFi-Kontrolle* enthält zwei Registerkarten, die nachfolgend beschrieben werden: Die Registerkarte *Allgemein*, auf der Sie angeben, welchen Verbindungsarten der Zugriff erlaubt ist, und die Registerkarte *Weiße Liste*, auf der Sie angeben, welchen spezifischen Netzen der Zugriff erlaubt ist. Wenn eine Verbindung auf keine der nachfolgend beschriebenen Weisen zugelassen wird, ist sie gesperrt.

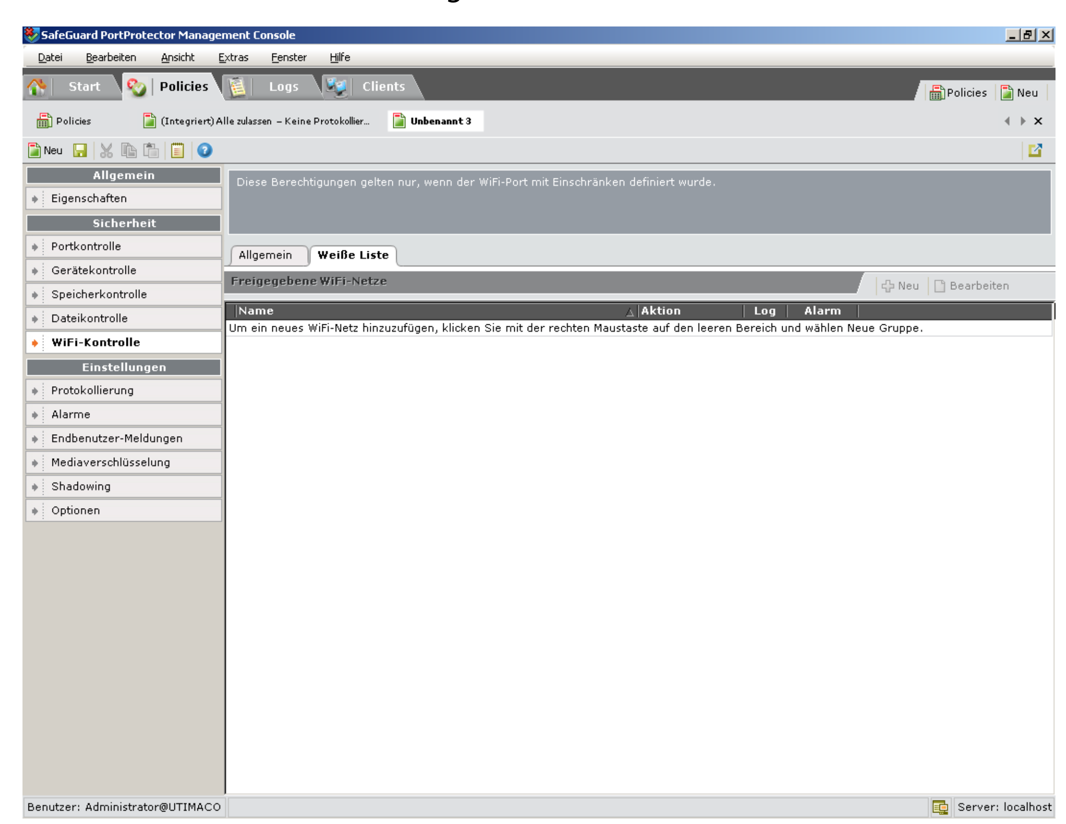
Darüber hinaus können Sie mit *WiFi-Kontrolle* Optionen für Aktivitätslog und Alarm bis auf die Ebene spezifischer Netze angeben. Das bedeutet: Sie können die Verbindung und Aktivität einiger WiFi-Verbindungen protokollieren, die Aktivitäten bestimmter zugelassener Netze aber nicht.

### 3.3.8.1 WiFi-Kontrolle – Registerkarte Allgemein

**WiFi-Verbindungsarten**: Mit dieser Option können Sie den Zugang zu WiFi-Netzen zulassen oder einschränken und Peer-to-Peer WiFi-Verbindungen zulassen oder sperren. Wenn Sie bei WiFi-Netzen **Einschränken** wählen, können Sie weitere Angaben darüber machen, welche Netze freigegeben sind.

Eine Beschreibung für die Definition der Einstellungen in diesem Fenster finden Sie in Definieren der WiFi-Kontrolle.

### 3.3.8.2 WiFi-Kontrolle – Registerkarte Weiße Liste




**Freigegebene WiFi-Netze:** Diese Option bezieht sich auf spezifische Netze, einschließlich deren Authentifizierungs- und Verschlüsselungseigenschaften.

Auf der rechten Seite der Registerkarte stehen drei Schaltflächen zur Verfügung:

- **Neue Gruppe** ( ): hiermit fügen Sie eine neue Gerätegruppe hinzu.
- **Gruppe bearbeiten** ( ): hiermit bearbeiten Sie eine Gerätegruppe.
- **Gruppe löschen** ( ): hiermit löschen Sie eine Gerätegruppe.

**Hinweis:** Dieses Fenster ist deaktiviert, wenn Sie die Option **Zulassen** für Netzwerke auf der Registerkarte *Allgemein* gewählt haben.

**Hinweis:** Falls ein Netz zu mehreren Gruppen gehört, und diese Gruppen dieselben Berechtigungen haben, wird SafeGuard PortProtector die Gruppen willkürlich auswählen. Wenn die Gruppen nicht dieselben Log- und Alarmeinstellungen haben, ist nicht vorhersehbar, welche Einstellungen angewendet werden.

Eine Beschreibung für die Definition der Einstellungen in diesem Fenster finden Sie in Definieren der WiFi-Kontrolle.

#### 3.3.8.3 Definieren der WiFi-Kontrolle

**So definieren Sie die WiFi-Kontrolle:**

1 Klicken Sie im Fenster *WiFi-Kontrolle* auf die Registerkarte *Allgemein*, sofern sie nicht aktiv ist.

2 Im Abschnitt *WiFi-Verbindungsarten* legen Sie in der Spalte *Aktion* die Berechtigungen für *WiFi-Netze (Infrastruktur)* wie folgt fest:

- **Zulassen ( ):** Lässt die Verbindung zu allen WiFi-Netzen zu.
- **Einschränken ( ):** Alle Netze sind gesperrt, es sei denn, sie sind auf der Registerkarte *Ausnahmen* speziell freigegeben, siehe auch *Freigeben von Geräten und WiFi-Verbindungen*.

3 Im Abschnitt *WiFi-Verbindungsarten* legen Sie in der Spalte *Aktion* die Berechtigungen für *Peer-to-Peer (Ad Hoc)* wie folgt fest:

- **Zulassen ( ):** Lässt alle Peer-to-Peer WiFi-Verbindungen zu.
- **Sperren ( ):** Sperrt alle Peer-to-Peer WiFi-Verbindungen.

Bei dieser Option sind keine feineren Berechtigungen verfügbar.

4 Markieren Sie das Kontrollkästchen **Log** für die einzelnen Verbindungstypen, wenn Verbindungsinitialisierungen bzw. -aktivitäten protokolliert werden sollen.

5 Markieren Sie das Kontrollkästchen **Alarm**, wenn Verbindungsinitialisierungen bzw. -aktivitäten einen Alarm auslösen sollen.

6 Wählen Sie bei **Freigegebenen Netze** die freigegebenen Netze, die Sie Ihrer weißen Liste hinzufügen möchten, siehe auch *Freigeben von Geräten und WiFi-Verbindungen.*

### 3.3.9 Schritt 9: Allgemeine Policy-Einstellungen definieren

Die allgemeinen Policy-Einstellungen dienen als Voreinstellung, wenn Sie keine policy-spezifischen Einstellungen angeben. Sie umfassen auch Log- and Alarmdefinitionen für Ereignisse, die nicht policy-spezifisch sind, wie etwa Manipulationsversuche, Policy-Aktualisierungen, Schutzaufhebung am SafeGuard PortProtector Client etc.

**Hinweis:** Das Modifizieren der allgemeinen Policy-Einstellungen ist optional. Wenn Sie SafeGuard PortProtector nur testen, ist es zu diesem Zeitpunkt eigentlich unnötig.

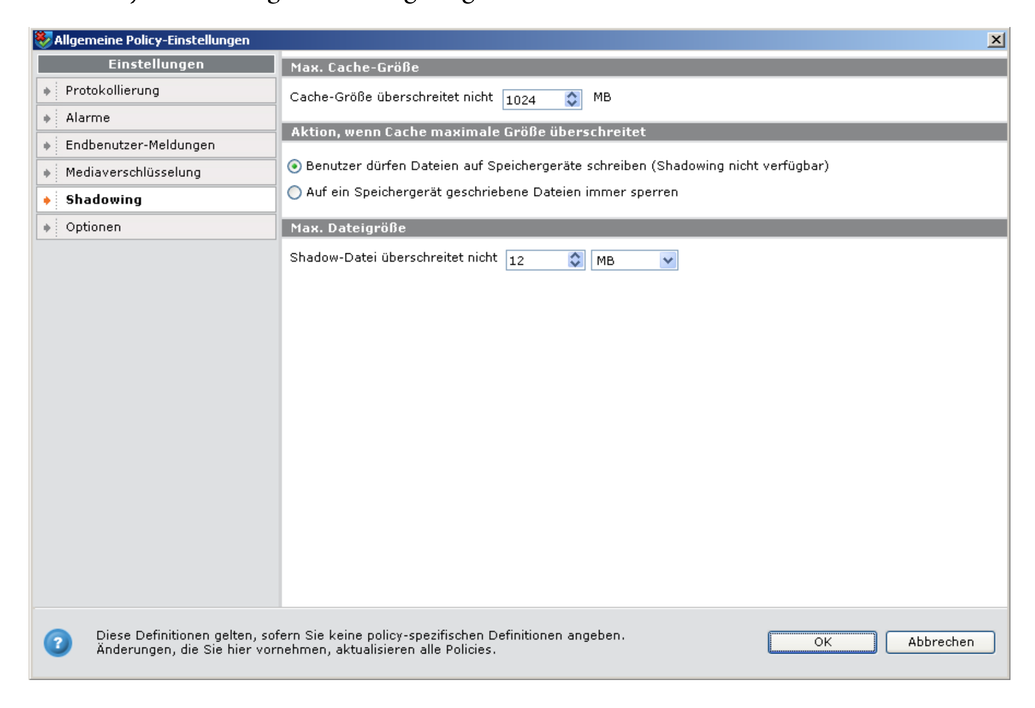
Da die Phasen der Schritte genau so definiert sind wie für die policy-spezifischen Einstellungen, folgen Sie bitte den nachstehenden Links zur Modifizierung der allgemeinen Policy-Einstellungen:

- *Definieren der Protokollierungseinstellungen*
- *Definieren der Alarmeinstellungen*
- *Definieren von Endbenutzer-Meldungen*
- *Definieren der Mediaverschlüsselungseinstellungen*
- *Definieren der Einstellungen für die Inhaltsprüfung*
- *Definieren der Einstellungen für Datei-Shadowing*
- *Definieren der Optionseinstellungen*

#### 3.3.9.1 Definieren der allgemeinen Policy-Einstellungen

**So definieren Sie die allgemeinen Policy-Einstellungen:**

1 Klicken Sie im Menü *Extras* auf **Allgemeine Policy-Einstellungen**. Das Fenster *Allgemeine Policy-Einstellungen* wird angezeigt:




2 Sie können dieses Fenster auch öffnen, indem Sie oben in den einzelnen Einstellungen-Fenstern auf **Allgemeine Policy-Einstellungen öffnen** klicken.

### 3.3.10 Schritt 10: Protokollierung definieren

Über diese Option werden die Protokollierungseinstellungen für die aktuelle Policy spezifiziert, wie etwa die Häufigkeit mit der Logs von einem geschützten Endpunkt an die SafeGuard PortProtector-Datenbank gesendet werden und deren Ziel.

Jeder Endpunkt, auf dem SafeGuard PortProtector Client installiert ist, sendet Logeinträge wie folgt:

- Sofort, wenn das Ereignis auftritt, oder
- periodisch, wie unten angegebenen

Wenn aus irgendeinem Grund keine Verbindung zwischen dem Endpunkt und dem SafeGuard PortProtector Management Server besteht, werden die Logeinträge auf dem Endpunkt gesammelt und gesendet, sobald die Kommunikation wieder hergestellt ist.

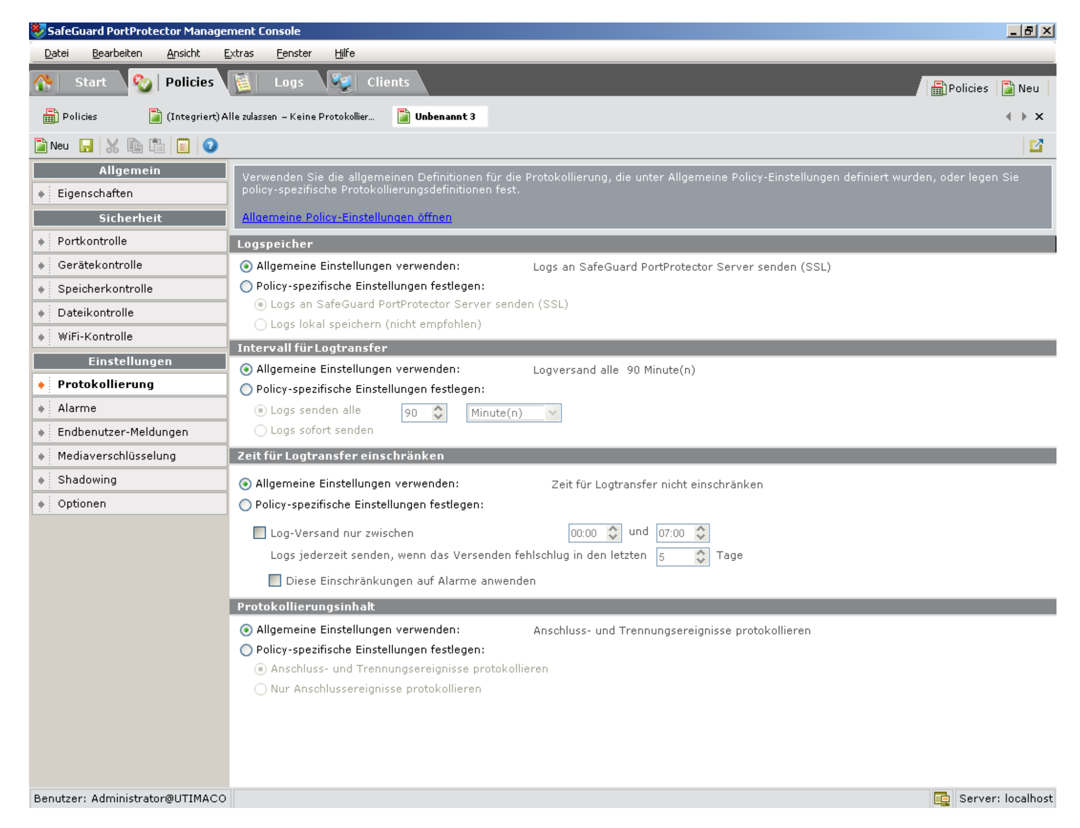
Sie können auch angeben, ob Trennungsereignisse protokolliert werden sollen.

**Hinweis:** Darüber hinaus können die meisten systemseitigen Protokollierungseinstellungen im Fenster Administration angegeben werden, siehe auch Konfigurieren *der Einstellungen auf der Registerkarte Logs und Alarme* im Kapitel *Administration*.

Die Protokollierungseinstellungen werden im Einstellungen-Fenster *Protokollierung* definiert.

**So öffnen Sie das Einstellungen-Fenster *Protokollierung*:**

Klicken Sie auf der linken Seite des Hauptfensters im Menü *Einstellungen* auf **Protokollierung**. Das Fenster *Protokollierung* wird angezeigt:



#### 3.3.10.1 Definieren der Protokollierungseinstellungen

**Hinweis:** Sie können in jedem Abschnitt dieses Fensters angeben, ob Sie die globalen Policy-Einstellungen verwenden möchten, indem Sie die Optionsschaltfläche **Allgemeine Einstellungen verwenden** aktivieren (um die globalen Policy-Einstellungen anzuzeigen oder zu bearbeiten, klicken Sie oben im Fenster auf Allgemeine Policy-Einstellungen öffnen).

Das Fenster enthält die folgenden Abschnitte:

- **Logspeicher:** Diese Einstellungen legen fest, wo die Logs gespeichert werden.
- **Intervall für Logtransfer:** Diese Einstellungen legen fest, ob die Logs sofort oder periodisch gesendet werden.
- **Zeit für Logtransfer einschränken:** Mit diesen Einstellungen können Sie die Log- and Alarmübertragung an den Management Server auf bestimmte Stunden beschränken.
- **Protokollierungsinhalt:** Diese Einstellungen legen fest, ob Verbindungs- und Trennungsereignisse oder nur Verbindungsereignisse protokolliert werden sollen.
- **Track offline use of devices:** In diesem Abschnitt können Sie die Nutzung verschlüsselter Geräte durch autorisierte Endbenutzer verfolgen, wenn sie nicht an das Organisationsnetz angeschlossen sind (siehe Verfolgung der Offline-Nutzung verschlüsselter Geräte im Kapitel *Endbenutzer-Erfahrung).*

**Hinweis:** Dieser Abschnitt wird nur im Fenster *Allgemeine Policy-Einstellungen* angezeigt.´

**So definieren Sie die Protokollierungseinstellungen:**

1. Klicken Sie im Abschnitt **Logspeicher** auf die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen** (ignorieren Sie diesen Schritt, wenn Sie globale Policy-Einstellungen definieren).
2. Wählen Sie eine der folgenden Optionsschaltflächen:

- **Logs an SafeGuard PortProtector Server senden (SSL):** Klicken Sie auf diese Option, um Logs über das sichere SSL-Protokoll an den SafeGuard PortProtector Management Server zu senden.
- **Logs lokal speichern (nicht empfohlen**): Auch wenn dies nicht zu empfehlen ist, können Sie auf diese Option klicken, um Logdatensätze lokal auf dem Endpunkt zu speichern und sie nie an den Management Server zu senden.

3. Klicken Sie im Abschnitt **Intervall für Logtransfer** auf die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen**.
4. Wählen Sie eine der folgenden Optionsschaltflächen:

- **Logs senden alle:** um Logs periodisch zu senden. Geben Sie die Anzahl und die Einheit für das gewünschte Intervall an.
- **Logs sofort senden:** um Logs sofort beim Auftreten eines Ereignisses zu senden.

**Hinweis:** Achten Sie bei der Konfiguration des *Log-Transferintervalls* besonders darauf, dass Ihr Netz und die Endpunkte nicht durch übermäßiges Versenden von Logs belastet werden.

Beachten Sie Folgendes:

- Die Anzahl der Endpunkte in Ihrem Netz
- Die Anzahl der erwarteten Ereignisse von den einzelnen Endpunkten (Client- und File-Logs)
- Der Bedarf an "Echtzeit"-Logdaten in der Management Console.

Während der Installation wird das Standard-Logintervall auf 90 Minuten gesetzt. Bei groß angelegten Deployments wenden Sie sich bitte an den Sophos Support, um Ihre Einstellungen zu optimieren.

5 Klicken Sie im Abschnitt **Zeit für Logtransfer einschränken** auf die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen**.

6 Markieren Sie das Kontrollkästchen **Log-Versand nur zwischen**, und geben Sie den gewünschten Zeitrahmen für das Versenden der Logs ein.

7 Wählen Sie die Anzahl der Tage, nach deren Ablauf das jederzeitige Senden von Logs aktiviert werden soll, falls während dieser Zeit keine Logs gesendet wurden.

8 Aktivieren Sie das Kontrollkästchen **Diese Einschränkungen auf Alarme anwenden**, wenn diese Einschränkung für Alarme gelten soll. (Alarmlogs werden normalerweise sofort gesendet. Wenn Sie dieses Kontrollkästchen markieren, werden Sie zur gleichen Zeit wie die Logs gesendet. Das Alarmereignis, wie etwa E-Mail-Benachrichtigung, erscheint sofort).

9 Klicken Sie im Abschnitt **Protokollierungsinhalt** auf die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen**.

10 Wählen Sie eine der folgenden Optionsschaltflächen:

- **Anschluss- und Trennungsereignisse protokollieren:** klicken Sie auf diese Option, um Verbindungs- und Trennungsereignisse zu protokollieren.
  Für alle zugelassenen Geräte, Speichergeräte und WiFi-Links wird jedes Mal ein Logeintrag aufgezeichnet, wenn das Gerät angeschlossen oder entfernt wird. Durch die Protokollierung von Trennungsereignissen können Sie anhand der Logs feststellen, wann und wie lange ein Gerät angeschlossen war.
- **Nur Anschlussereignisse protokollieren:** Klicken Sie auf diese Option, wenn Sie Verbindungsereignisse protokollieren wollen.

11 Aktivieren Sie das Kontrollkästchen im Abschnitt **Track Offline Use of Devices**, um die Offline-Nutzung verschlüsselter Geräte zu protokollieren.

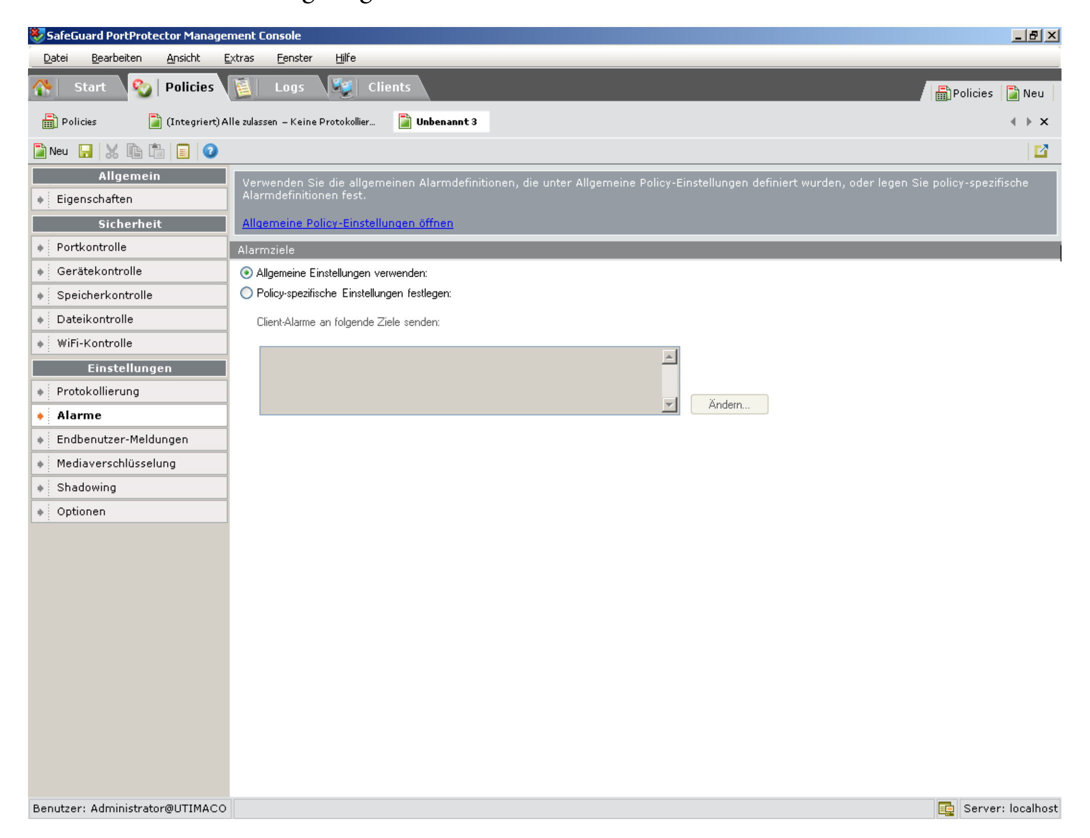
**Hinweis:** Dieser Abschnitt wird nur im Fenster *Allgemeine Policy-Einstellungen* angezeigt.

## 3.3.11 Schritt 11: Alarme definieren

Im Einstellungen-Fenster *Alarme* wählen Sie die Alarmziele des Clients aus.

**So öffnen Sie das Einstellungen-Fenster *Alarme*:**

Klicken Sie auf der linken Seite des Hauptfensters im Menü *Einstellungen* auf **Alarme**. Das Fenster *Alarme* wird angezeigt:



#### 3.3.11.1 Definieren der Alarmeinstellungen

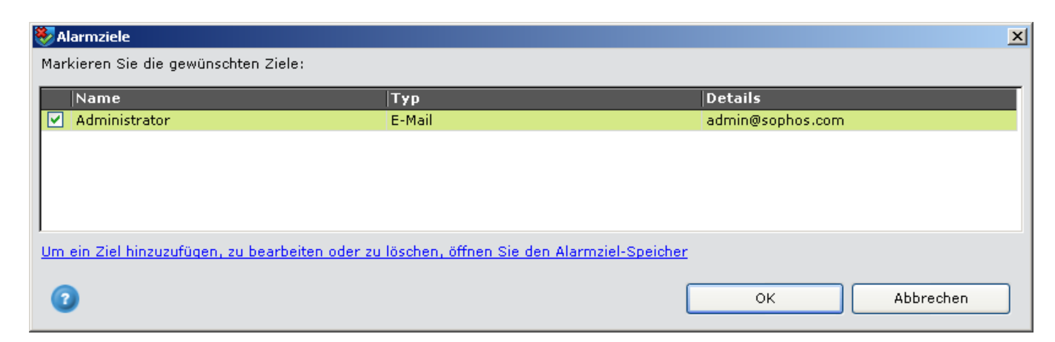
Hinweis: Sie können wählen, ob Sie die globalen Policy-Einstellungen verwenden möchten, indem Sie die Optionsschaltfläche **Allgemeine Einstellungen verwenden** aktivieren (um die allgemeinen Policy-Einstellungen anzuzeigen oder zu bearbeiten, klicken Sie oben im Fenster auf Allgemeine Policy-Einstellungen öffnen).

**So definieren Sie Alarmeinstellungen:**

1 Im Abschnitt **Client Events** geben Sie an, für welche Administrations- und Manipulationsereignisse eine Logs/Alarme generiert werden sollen (ignorieren Sie diesen Schritt, wenn Sie nicht die globalen Policy-Einstellungen definieren).

2 Aktivieren Sie die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen.** Falls zuvor Alarmziele definierte wurden, werden sie in der Zielliste angezeigt. Ansonsten ist die Liste leer ((ignorieren Sie diesen Schritt, wenn Sie globale Policy-Einstellungen definieren).

3 Klicken Sie auf **Ändern.** Das Fenster *Alarmziele* wird angezeigt, in dem alle verfügbaren Alarmziele aufgelistet werden, die zuvor unter Alert Destination Repository definiert wurden (siehe *Alarmziel Speicher* im Kapitel *Administration*).




4 Aktivieren bzw. deaktivieren Sie die Ziele wie gewünscht, und klicken Sie auf **OK.**

Hinweis: Informationen zum Hinzufügen, Bearbeiten und Löschen eines Ziels finden Sie in *Alarmziel Speicher* im *Alarmziel Speicher* im Kapitel *Administration.*

### 3.3.12 Schritt 12: Endbenutzer-Meldungen definieren

Sobald eine SafeGuard PortProtector-Policy zugeordnet ist, zeigt der SafeGuard PortProtector Client dem Endbenutzer bei verschiedenen Situationen eine Ereignismeldung an, beispielsweise wenn der Versuch einer Policy-Verletzung festgestellt wird oder eine Maßnahme seitens des Endbenutzers erforderlich ist.

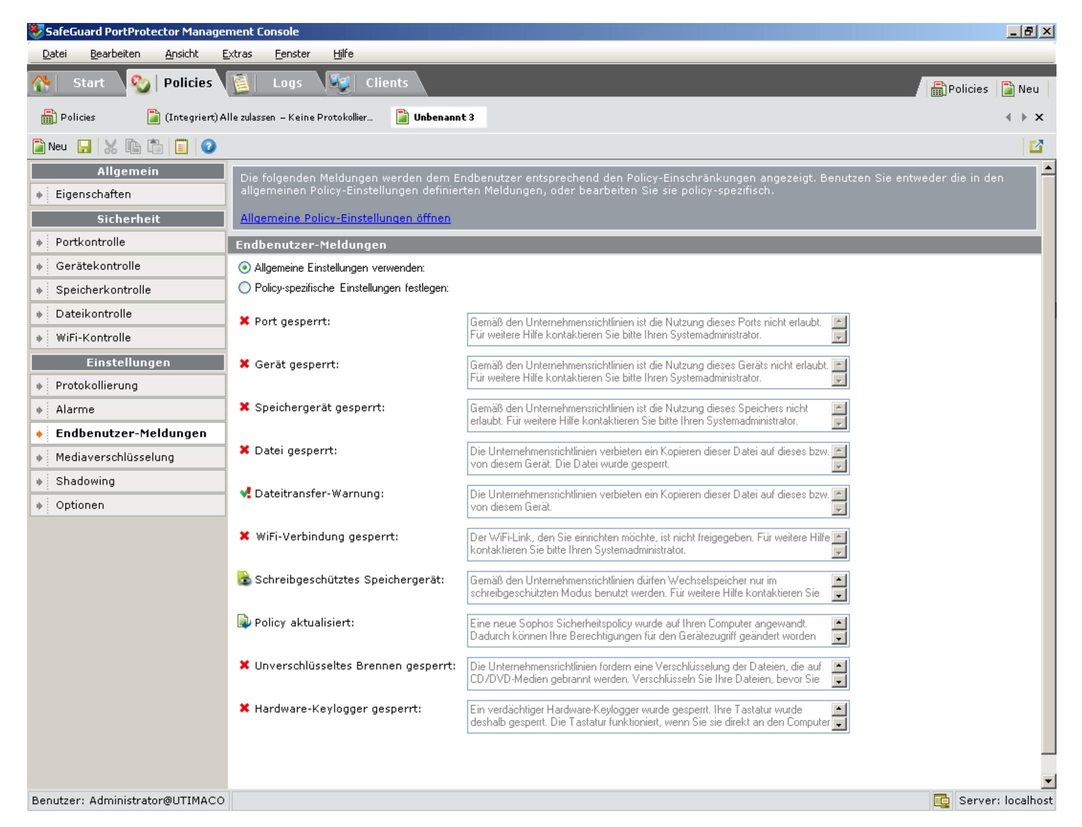
SafeGuard PortProtector Client wird mit Standardmeldungen geliefert, die Sie über die Option **Endbenutzer-Meldungen** im Menü *Einstellungen* auf der linken Seite des Hauptfensters ändern können.

Hinweis: Im Abschnitt *Meldungen des SafeGuard PortProtector Clients* finden Sie eine Beschreibung, wie und wann diese Meldungen auf den Endpunkten erscheinen.

Die Einstellungen für die Endbenutzer-Meldungen werden im Settings-Fenster *Endbenutzer-Meldungen* definiert.

**So öffnen Sie das Einstellungen-Fenster *Endbenutzer-Meldungen*:**

Klicken Sie auf der linken Seite des Hauptfensters im Menü *Einstellungen* auf **Endbenutzer-Meldungen**. Das Fenster *Endbenutzer-Meldungen* wird angezeigt:



#### 3.3.12.1 Definieren von Endbenutzer-Meldungen

**Hinweis:** Sie können auswählen, ob Sie die globalen Policy-Einstellungen verwenden möchten, indem Sie die Optionsschaltfläche **Allgemeine Einstellungen verwenden** aktivieren (um die allgemeinen Policy-Einstellungen anzuzeigen oder zu bearbeiten, klicken Sie oben im Fenster auf Allgemeine Policy-Einstellungen öffnen).

**So definieren Sie die Einstellungen für Endbenutzer-Meldungen:**

1 Aktivieren Sie die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen** (ignorieren Sie diesen Schritt, wenn Sie allgemeine Policy-Einstellungen definieren).

2 Bearbeiten Sie die Meldungen wie folgt:

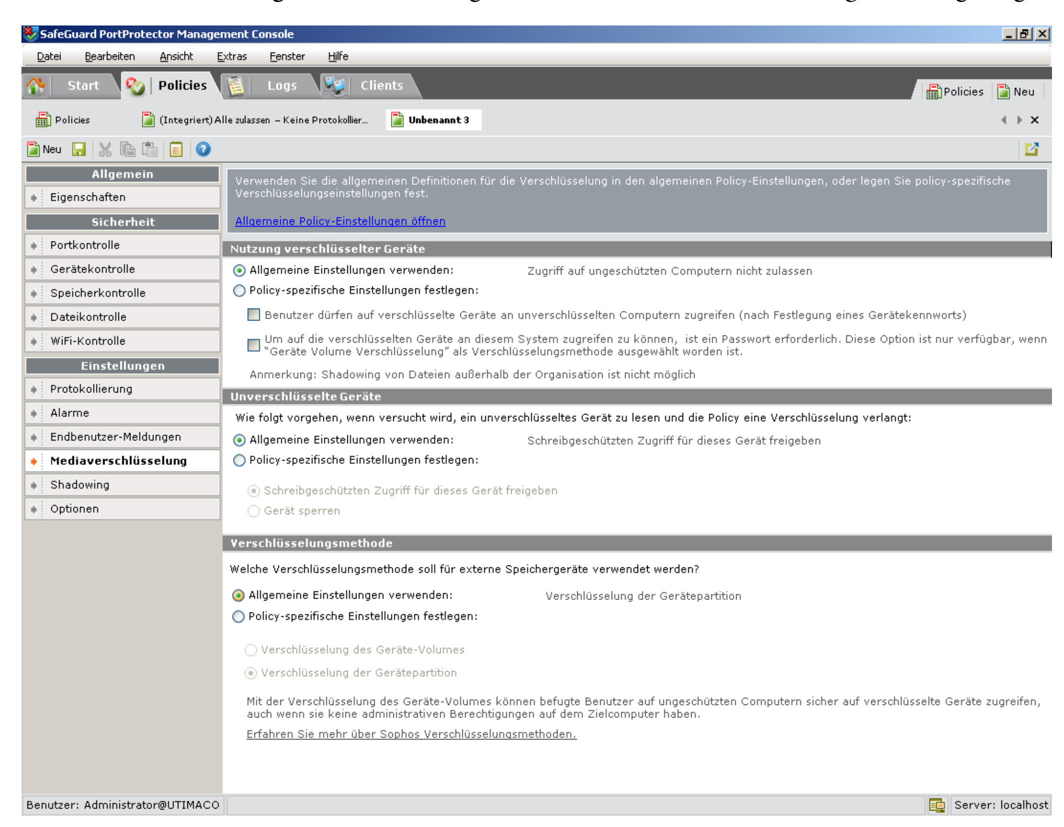
- **Port gesperrt:** Diese Meldung wird angezeigt, wenn ein Computer versucht, auf einen **blockierten** Port zuzugreifen. Bei integrierten Ports wird diese Meldung angezeigt, wenn der Endpunkt-Computer neu startet und versucht, den Port zu initialisieren. Sie wird auch angezeigt, wenn ein Adapter für diesen Port an den Endpunkt angeschlossen ist.
- **Gerät gesperrt:** Diese Meldung wird angezeigt, wenn versucht wird, ein nicht freigegebenes Gerät über einen **eingeschränkten** Port anzuschließen.
- **Speichergerät gesperrt:** Diese Meldung wird angezeigt, wenn versucht wird, ein nicht freigegebenes Speichergerät anzuschließen.
- **Datei gesperrt:** Diese Meldung wird angezeigt, wenn der Endbenutzer versucht, eine Datei auf ein Speichergerät zu schreiben bzw. davon zu lesen, deren Typ gesperrt ist.
- **Dateitransfer-Warnung:** Diese Meldung wird angezeigt, wenn eine Datei mit sensiblem Inhalt auf ein Speichergerät geschrieben wird.
- **WiFi-Verbindung gesperrt:** Diese Meldung wird angezeigt, wenn versucht wird, eine nicht freigegebene WiFi-Verbindung herzustellen.
- **Schreibgeschütztes Speichergerät:** Diese Meldung wird angezeigt, wenn ein auf **Schreibgeschützt** gesetztes Speichergerät angeschlossen wird. Diese Meldung besagt, dass Sie von diesem Speichergerät lesen, aber nicht darauf schreiben können.
- **Policy aktualisiert:** Diese Meldung wird angezeigt, wenn dem Endpunkt eine neue Policy zugewiesen wird.
- **Format Encrypted Device:** Diese Meldung wird angezeigt, wenn die Policy ein verschlüsseltes Wechselspeichermedium fordert und ein unverschlüsseltes Gerät entdeckt wird (siehe *Verschlüsseln eines Geräts* in *Kapitel 9, Endbenutzer-Erfahrung*).
- **Hardware-Keylogger gesperrt:** Diese Meldung wird angezeigt, wenn versucht wird, einen Hardware-Keylogger anzuschließen und Hardware-Keylogger auf **Gesperrt** gesetzt sind.

## 3.3.13 Schritt 13: Mediaverschlüsselung definieren

Die Verschlüsselungseinstellungen bestimmen das Verhalten des Systems, wenn die Berechtigungen eines Wechselspeichergeräts eine Verschlüsselung erforderlich machen. Die Verschlüsselungseinstellungen werden im Einstellungsfenster *Mediaverschlüsselung* definiert.

**So öffnen Sie das Einstellungen-Fenster *Mediaverschlüsselung*:**

Klicken Sie auf der linken Seite des Hauptfensters im Menü *Einstellungen* auf **Mediaverschlüsselung.** Das Einstellungen-Fenster *Mediaverschlüsselung* wird angezeigt:




### 3.3.13.1 Definieren der Mediaverschlüsselungseinstellungen

Hinweis: Sie können in jedem Abschnitt dieses Fensters angeben, ob Sie die globalen Policy-Einstellungen verwenden möchten, indem Sie die Optionsschaltfläche **Allgemeine Einstellungen verwenden** aktivieren (um die globalen Policy-Einstellungen anzuzeigen oder zu bearbeiten, klicken Sie oben im Fenster auf Allgemeine Policy-Einstellungen öffnen).

Das Fenster enthält die folgenden Abschnitte:

- **Nutzung verschlüsselter Geräte:** Die Einstellungen in diesem Abschnitt legen fest, ob die Benutzer auf organisatorisch verschlüsselte Wechselspeichergeräte auf organisationsfremden Computern mit vollem Zugriff oder schreibgeschützten Zugriff zugreifen dürfen (siehe *Offline-Zugriff auf verschlüsselte Geräte* in *Kapitel 9, Endbenutzer-Erfahrung).* Auch, ob man auf verschlüsselte Wechselspeichergeräte selbst in der Organisation zugreifen kann, d. h. ein Kennwort für den Zugriff erforderlich ist (siehe *Online-Zugriff auf verschlüsselte Geräte*).
- **Unverschlüsselte Geräte:** In diesem Abschnitt können Sie das Verhalten festlegen, wenn die Policy eine Verschlüsselung fordert und ein unverschlüsseltes Gerät entdeckt wird. Das Gerät kann entweder gesperrt oder schreibgeschützt zugelassen werden.

- **Verschlüsselungsmethode:** In diesem Abschnitt legen Sie die Methode der Verschlüsselung von Wechselspeichergeräten fest. Dadurch wird auch beeinflusst, inwieweit befugte Benutzer auf die verschlüsselten Speichergeräte außerhalb der Organisation zugreifen können, siehe auch *Verschlüsselung und Entschlüsselung von Wechselspeichergeräten* in *Kapitel 9, Endbenutzer-Erfahrung*. Der Unterschied zwischen den beiden Verschlüsselungsmethoden ist in *Methoden der Media-Verschlüsselung* beschrieben.

**So definieren Sie Verschlüsselungseinstellungen:**

1. Klicken Sie im Abschnitt *Nutzung verschlüsselter Geräte* auf die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen** (ignorieren Sie diesen Schritt, wenn Sie allgemeine Policy-Einstellungen definieren).

2. Wenn Sie zulassen möchten, dass Benutzer auf organisatorisch verschlüsselte Geräte zugreifen können, wenn sie sich nicht im Organisationsnetz befinden, aktivieren Sie das Kontrollkästchen **Benutzer dürfen auf unverschlüsselte Geräte an unverschlüsselten Computern zugreifen.**

3. Aktivieren Sie die entsprechende Optionsschaltfläche, um festzulegen, ob der Benutzer **vollen Zugriff** oder **schreibgeschützten Zugriff** haben wird.

4. Wenn Sie den Benutzerzugriff auf verschlüsselte Geräte im Organisationsnetz einschränken möchten, aktivieren Sie das Kontrollkästchen **Benutzer müssen Kennwort eingeben, um auf verschlüsselte Geräte an geschützten Computern zugreifen zu können.**
   Diese Option ist nur dann verfügbar, wenn Sie sowohl **Benutzer dürfen auf verschlüsselte Geräte an unverschlüsselten Computern zugreifen** als auch **Verschlüsselung des Geräte-Volumes** als *Verschlüsselungsmethode* gewählt haben.

5. Klicken Sie im Abschnitt *Unverschlüsselte Geräte* auf die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen.**

6. Wählen Sie die entsprechende Optionsschaltfläche je nachdem, ob Sie unverschlüsselte Geräte sperren oder den Benutzern schreibgeschützten Zugriff auf solche Geräte gewähren möchten.

7. Wählen Sie die entsprechende Optionsschaltfläche **Verschlüsselung des Geräte-Volumes** (Voreinstellung) oder **Verschlüsselung der Gerätepartition** um die Methode für die Gewährung des Offline-Zugriffs auf Wechselspeichergeräte durch befugte Benutzer festzulegen.

**Hinweis für Systemadministratoren:** Endbenutzer mit einer gültigen Policy, die eine Verschlüsselung der Wechselspeichergeräte erfordert, müssen über die Anforderungen in *Verschlüsselung und Entschlüsselung von Wechselspeichergeräten* in *Kapitel 9, Endbenutzer-Erfahrung* informiert werden, da der Client möglicherweise Meldungen anzeigt, die sie zur Verschlüsselung der Wechselspeichergeräte auffordern.

#### 3.3.13.1.1 Methoden der Mediaverschlüsselung

SafeGuard PortProtector bietet zwei Methoden zur Verschlüsselung von Wechselspeichergeräten. Die eingesetzte Verschlüsselungsmethode beeinflusst, inwieweit befugte Benutzer auf die verschlüsselten Speichergeräte sowohl innerhalb als auch außerhalb der Organisation zugreifen können, siehe auch *Verschlüsselung und Entschlüsselung von Wechselspeichergeräten* in *Kapitel 9, Endbenutzer-Erfahrung.*

- **Verschlüsselung des Geräte-Volumes:** Diese Verschlüsselungsmethode ermöglicht den Zugriff auf Speichergeräte durch befugte Benutzer außerhalb der Organisation, **ohne** dazu lokale Administrationsrechte zu benötigen. Jedoch ist der Zugriff auf Dateien für den Benutzer weniger intuitiv als bei der Option **Verschlüsselung der Gerätepartition** (Beschreibung siehe unten). Das Wechselspeichergerät zeigt zwei Dateien: das Access Secure Data Utility und einen Container mit den verschlüsselten Dateien.

**Hinweis:** Löschen Sie den Container der verschlüsselten Dateien nicht vom Wechselspeichergerät. Durch das Löschen des Containers werden alle darin gespeicherten Daten gelöscht.

- **Verschlüsselung der Gerätepartition (Voreinstellung):** Diese Verschlüsselungsmethode ermöglicht den Zugriff auf Speichergeräte durch befugte Benutzer außerhalb der Organisation, **allerdings** benötigen sie dazu lokale Administrationsrechte auf dem ungeschützten Computer. Der Zugriff auf die Dateien ist für den Benutzer einfacher als bei der Option **Verschlüsselung des Geräte-Volumes** (Beschreibung siehe oben).

**Hinweis:** Das oben Genannte gilt nur für Wechselspeichergeräte. Die Methode der Geräte-Volume-Verschlüsselung wird standardmäßig für CD/DVD und externe Festplattenlaufwerke angewandt.

## 3.3.14 Schritt 14: Inhaltsprüfung definieren

Wenn die Funktion der Inhaltsprüfung aktiviert ist, definieren Sie in diesem Schritt die entsprechenden Einstellungen, z. B. ob Alarme ausgegeben werden sollen, die maximale Größe für den Datei-Cache etc.

### 3.3.14.1 Definieren der Einstellungen für die Inhaltsprüfung

Da dieser Schritt nur von Benutzern ausgeführt wird, bei denen Safend Protector mit einer Inhaltsprüfungslösung eines Drittanbieters integriert ist, wird das Verfahren getrennt beschrieben.

## 3.3.15 Schritt 15: Einstellungen für Datei-Shadowing definieren

Datei-Shadowing bietet die Möglichkeit der Rückverfolgung und Erfassung von Kopien von Dateien, die zu/von externen Speichergeräten verschoben wurden. Dadurch sind Sicherheitsbeauftragte in der Lage, Sicherheitsverletzungen zu lokalisieren und zu identifizieren. Sie können zudem forensische Beweise analysieren, die Wichtung bestimmen und entsprechende Maßnahmen ergreifen.

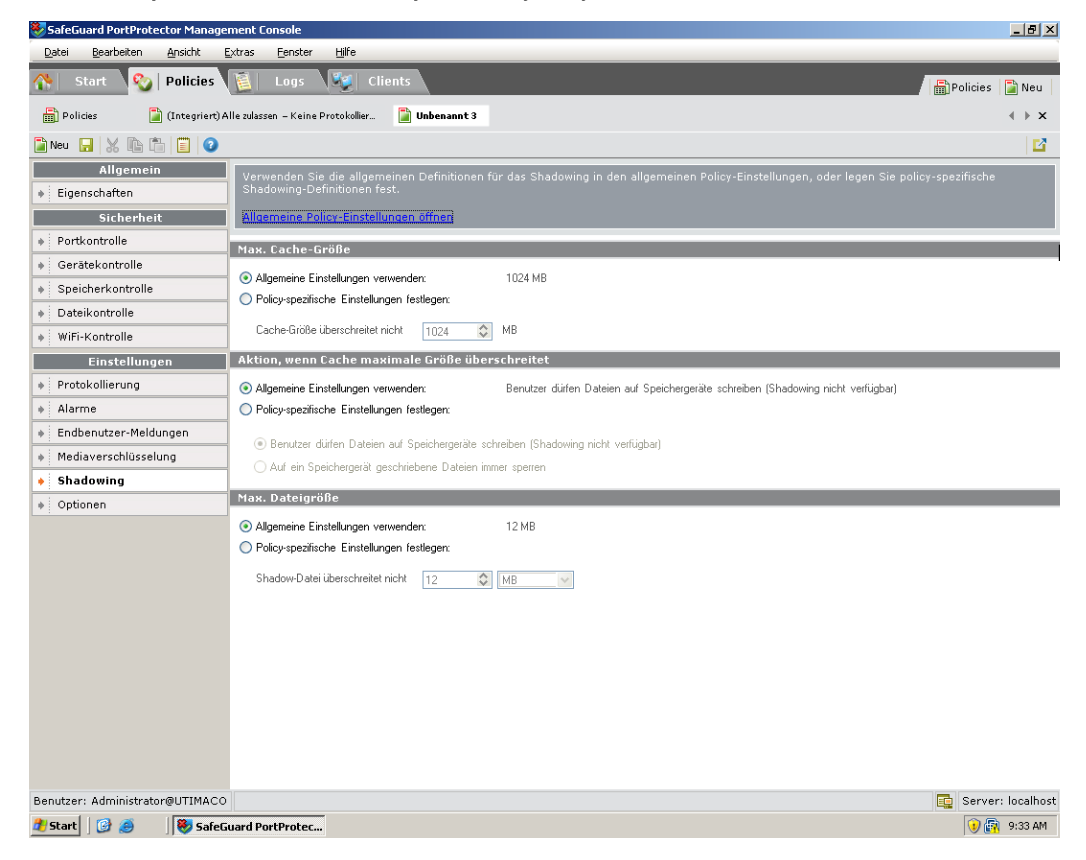
Die 'Shadow'-Dateien werden sicher von den Endpunkten an den Server gesendet und in einem zentralen Speicher abgelegt. Diese Dateien stehen zur Überprüfung durch befugte Administratoren mit **Shadow-Dateien einsehen**-Berechtigung zur Verfügung. Die Shadow-Dateien werden mit ihrem ursprünglichen Dateinamen und in ihrem ursprünglichen Format gespeichert.

Ein Administrator kann ein oder mehrere Netzsegmente als zentralen Speicher für das File-

Shadowing definieren. Wenn mehrere Netzsegmente definierte werden, wird ein Lastausgleichsalgorithmus genutzt, um sicherzustellen, dass die Last auf alle Teile gleichmäßig verteilt wird.

**So öffnen Sie das Einstellungen-Fenster Shadowing:**

Klicken Sie auf der linken Seite des Hauptfensters im Menü *Einstellungen* auf **Shadowing.** Das Einstellungen-Fenster Shadowing wird angezeigt:



### 3.3.15.1 Definieren der Einstellungen für Datei-Shadowing

**Hinweis:** Sie können in jedem Abschnitt dieses Fensters auswählen, ob Sie die globalen Policy-Einstellungen verwenden möchten, indem Sie die Optionsschaltfläche **Allgemeine Einstellungen verwenden** aktivieren (um die globalen Policy-Einstellungen anzuzeigen oder zu bearbeiten, klicken Sie oben im Fenster auf *Allgemeine Policy-Einstellungen öffnen*).

Dieses Fenster enthält folgende Abschnitte:

- **Max Cache-Größe:** Die Einstellungen in diesem Abschnitt legen die maximale Größe des lokalen Cache-Speichers fest, in den die Shadow-Dateien geschrieben werden. Ähnlich wie bei der Protokollierung werden Shadow-Dateien lokal auf dem geschützten Computer gespeichert, bis sie auf einen Server geleitet werden.

**Hinweis:** Auf Laptops wird eventuell mehr Speicherplatz für diesen lokalen Cache benötigt, da sie – im Gegensatz zu Desktop-Computern – einen Großteil der Zeit außerhalb des Organisationsnetzes benutzt werden.

- **Aktion, wenn Cache maximale Größe überschreitet:** Über die Einstellungen in diesem Abschnitt werden die Maßnahmen festgelegt, die von SafeGuard PortProtector ergriffen werden sollen, wenn der lokal Cache die im Bereich **Max Cache-Größe** definierte Größe überschreitet.
- **Max. Dateigröße:** Dieser Bereich legt die maximale Größe der Shadow-Dateien fest. Dateien, die diese Größe überschreiten, werden nicht kopiert.

**So definieren Sie die Einstellungen für das Datei-Shadowing:**

1. Geben Sie im Abschnitt *Max. Cache-Größe* im Feld *Cache-Größe überschreitet nicht* die maximale Größe des lokalen Caches in MB an. Wenn dieser Cache zu voll wird, handelt SafeGuard PortProtector gemäß den oben beschriebenen Maßnahmen.
2. Aktivieren Sie im Bereich *Aktion, wenn Cache maximale Größe überschreitet* eine der beiden folgenden Optionsschaltflächen:

- **Benutzer dürfen Dateien auf Speichergeräte schreiben (Shadowing nicht verfügbar):** Wenn der (oben definierte) lokale Cache voll wird, lässt SafeGuard PortProtector alle auf das Speichergerät geschriebenen Dateien zu.
- **Auf ein Speichergerät geschriebene Dateien immer sperren:** Wenn der (oben definierte) lokale Cache voll wird, blockiert SafeGuard PortProtector alle auf das Speichergerät geschriebenen Dateien. Durch die Auswahl dieser Option stellen Sie sicher, dass keine Dateien von dem geschützten Computer übertragen werden, ohne dass sie durch das Shadowing kopiert werden.

3. Geben Sie im Abschnitt *Max. Dateigröße* im Feld *Shadow-Datei überschreitet nicht* die maximale Größe für eine Shadow-Datei in MB an. Größere Dateien werden nicht kopiert.

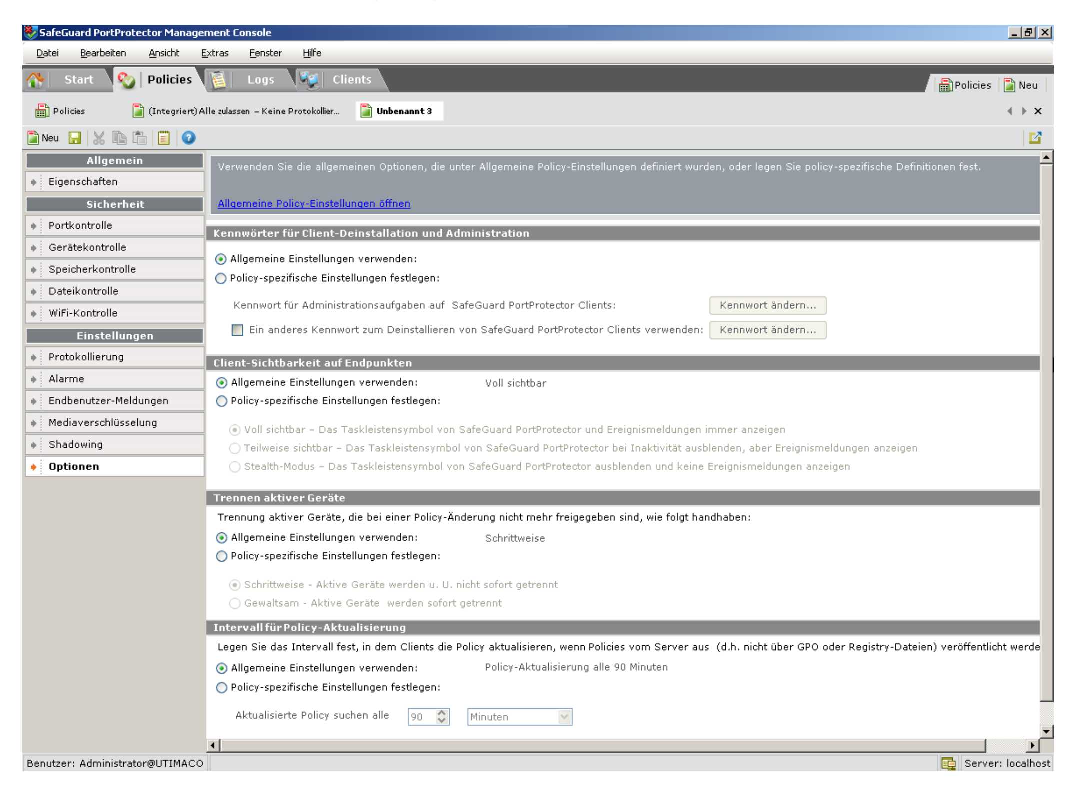
## 3.3.16 Schritt 16: Optionen definieren

Mit dem **Optionen**-Aspekt einer Policy können Sie verschiedene Verhaltensaspekte von SafeGuard PortProtector Client auf den Endpunkten definieren. Dazu gehören Kennworteinstellungen, Anzeigeeinstellungen für Taskleistensymbole und die Definitionen von Methoden für das Trennen aktiver Geräte, falls dies erforderlich werden sollte.

Die Optionseinstellungen werden im Einstellungen-Fenster *Optionen* definiert.

**So öffnen Sie das Einstellungen-Fenster *Optionen*:**

Klicken Sie auf der linken Seite des Hauptfensters im Menü *Einstellungen* auf **Optionen**. Das Fenster *Optionen* wird angezeigt:



### 3.3.16.1 Definieren der Optionseinstellungen

**Hinweis:** Sie können in jedem Abschnitt dieses Fensters angeben, ob Sie die globalen Policy-Einstellungen verwenden möchten, indem Sie die Optionsschaltfläche **Allgemeine Einstellungen verwenden** aktivieren (um die allgemeinen Policy-Einstellungen anzuzeigen oder zu bearbeiten, klicken Sie oben im Fenster auf Allgemeine Policy-Einstellungen öffnen).

Das Fenster enthält die folgenden Abschnitte:

- ***Kennwörter für Client-Deinstallation und Administration***: Die Einstellungen in diesem Abschnitt legen die Kennwörter fest, die bei der Verwaltung bzw. Deinstallation von SafeGuard PortProtector Client benutzt werden.
- ***Client-Sichtbarkeit auf Endpunkten***: Die Einstellungen in diesem Abschnitt legen fest, ob und wann das Taskleistensymbol und die Ereignismeldungen des SafeGuard PortProtector Client angezeigt werden.
- ***Trennen aktiver Geräte***: Die Einstellungen in diesem Abschnitt legen fest, wie SafeGuard PortProtector Geräte trennt, die früher zugelassen waren, aber jetzt nicht mehr freigegeben sind.
- ***Intervall für Policy-Aktualisierung:*** Die Einstellungen in diesem Abschnitt legen das Intervall fest, in dem Clients ihre Policy aktualisieren, wenn die Policies direkt vom Management Server (d. h. Policy-Server) verteilt werden.

**Hinweis:** Dieser Abschnitt wird auf der Seite *Optionen* nur dann angezeigt, wenn der Policy-Server zur Policy-Verteilung genutzt wird (d. h. entweder alleine, oder zusätzlich zu GPO oder Registry-Dateien).

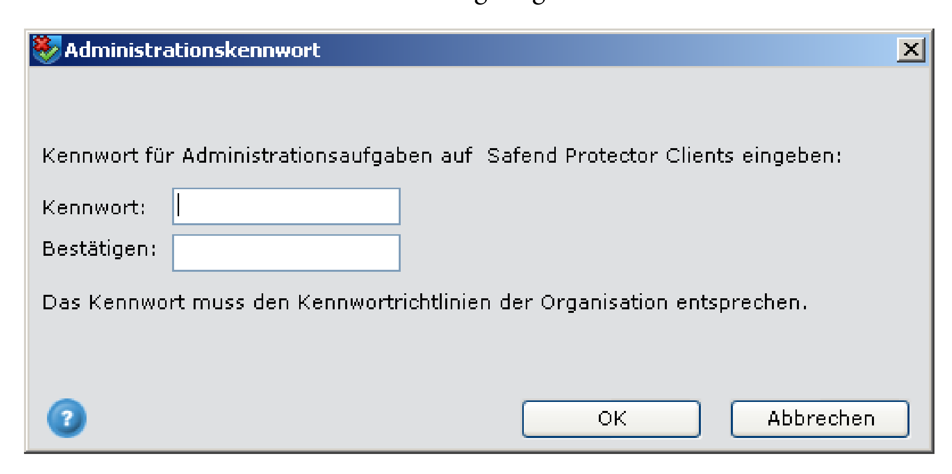
#### 3.3.16.1.1 Kennwort für Client-Administration

Hierbei handelt es sich um das Kennwort zur Ausführung von Administratorsaufgaben auf SafeGuard PortProtector Clients. Hierzu gehören auch das Aufheben und Deinstallieren des Clients. Sie legen das Kennwort im Fenster *Administrationskennwort* fest.

**So öffnen Sie das Fenster:**

1 Klicken Sie im Abschnitt Kennwörter für Client-Deinstallation und Administration auf die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen** (ignorieren Sie diesen Schritt, wenn Sie allgemeine Policy-Einstellungen definieren).

2 Klicken **Sie neben dem Kennwort** für die Ausführung von Administrationsaufgaben auf dem SafeGuard PortProtector Client auf die Schaltfläche **Kennwort ändern**. Das Fenster Administrationskennwort wird angezeigt:



#### 3.3.16.1.1.1 Definieren des Kennworts für die Client-Administration

So definieren Sie ein Kennwort für die Client-Verwaltung:

1 Geben Sie in diesem Fenster das Kennwort für die Ausführung von Administratorsaufgaben auf SafeGuard PortProtector Clients ein und bestätigen Sie es. Das Kennwort muss den Kennwortregeln in Ihrer Organisation entsprechen.

2 Klicken Sie auf **OK**.

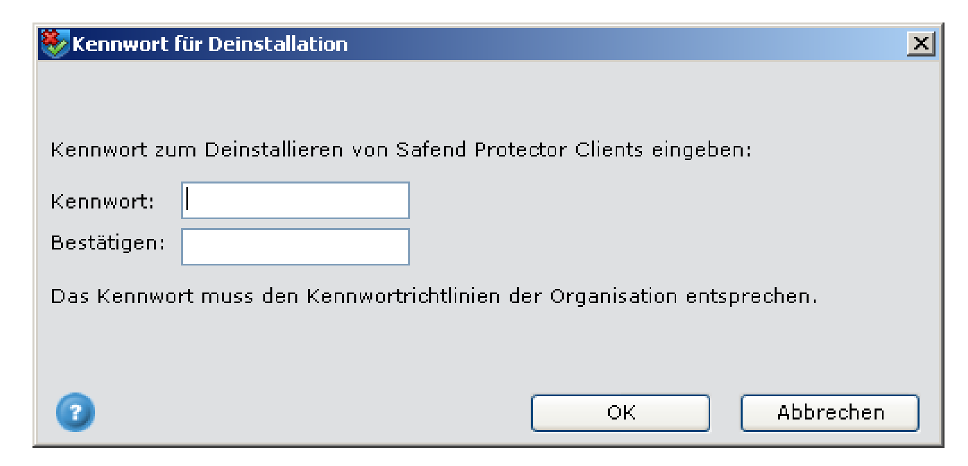
### 3.3.16.1.2 Client-Kennwort für Deinstallation

Hierbei handelt es sich um das Kennwort für die Deinstallation von SafeGuard PortProtector Clients von Endpunkten, für den Fall, dass Sie ein anderes Kennwort als das Administrationskennwort verwenden möchten. Sie legen das Kennwort im Fenster Kennwort für Deinstallation fest.

**So öffnen Sie das Fenster:**

Aktivieren Sie im Abschnitt *Kennwörter für Client-Deinstallation und Administration* das Kontrollkästchen neben *Ein anderes Kennwort zum Deinstallieren von SafeGuard PortProtector Clients verwenden*.

Klicken Sie auf die daneben befindliche Schaltfläche **Kennwort ändern**. Das Fenster *Kennwort für Deinstallation* wird angezeigt:




#### 3.3.16.1.2.1 Definieren des Kennworts für die Client-Deinstallation

1 Geben Sie in diesem Fenster das Kennwort für die Deinstallation von SafeGuard PortProtector Clients von Endpunkten ein und bestätigen Sie es. Das von Ihnen festgelegte Kennwort muss den Kennwortregeln in Ihrer Organisation entsprechen.

2 Klicken Sie auf **OK**.

**Hinweis:** Bei der Installation des Produkts sind beide Kennwörter auf "**Password1**" gesetzt. Da das Kennwort einer der Grundpfeiler für die Manipulationssicherheit des Clients ist, wird dringend empfohlen, das Kennwort zu ändern sobald Sie mit dem Deployment des Produkts in einer Produktionsumgebung beginnen.

#### 3.3.16.1.3 Definieren der Client-Sichtbarkeit auf Endpunkten

Die Einstellungen in diesem Abschnitt legen fest, ob und wann das Taskleistensymbol und die Ereignismeldungen des SafeGuard PortProtector Client angezeigt werden.

1 Klicken Sie im Abschnitt *Client-Sichtbarkeit auf Endpunkten* auf die Optionsschaltfläche **Policy-spezifische Einstellungen festlegen**.

2 Wählen Sie eine der folgenden Optionsschaltflächen:

- **Voll sichtbar:** Wenn Sie diese Option wählen, wird das SafeGuard PortProtector-Symbol immer in der Taskleiste angezeigt, auch wenn der SafeGuard PortProtector Client untätig ist. Außerdem werden Ereignismeldungen angezeigt. In diesem Fall ist SafeGuard PortProtector für den Endbenutzer erkennbar.
- **Teilweise sichtbar**: Wenn Sie diese Option wählen, wird das SafeGuard PortProtector-Symbol ausgeblendet, wenn der Client untätig ist. Sobald ein Ereignis eintritt, werden das Symbol und die Ereignismeldung kurz eingeblendet und verschwinden dann wieder.
- **Stealth-Modus:** Wenn Sie diese Option wählen, werden das SafeGuard PortProtector-Symbol und Ereignismeldungen niemals angezeigt. Diese Option kann genutzt werden, wenn Sie verhindern möchten, dass die Benutzer über den Einsatz von SafeGuard PortProtector auf ihrem Computer Bescheid wissen.

#### 3.3.16.1.4 Definieren der Trennung aktiver Geräte

Manchmal ist ein Gerät an einen Computer angeschlossen, für den eine neue Policy zur Anwendung kommt, die dieses Gerät nicht mehr zulässt. In einem solchen Fall verlangt der SafeGuard PortProtector Client vom Betriebssystem die Trennung des Geräts. Wenn das Gerät benutzt wird, kann es vorkommen, dass das Betriebssystem nicht dazu in der Lage ist. Die Einstellungen in diesem Abschnitt legen fest, wie SafeGuard PortProtector in diesem Fall das nicht mehr freigegebene Gerät trennt.

1 Klicken Sie im Abschnitt *Disconnecting Active Devices* auf die Optionsschaltfläche **Policy-spezifische Einstellungen definieren**.

2 Wählen Sie eine der folgenden Optionsschaltflächen:

- **Schrittweise:** Wenn Sie diese Option wählen, trennt auch SafeGuard PortProtector keine Geräte, die das Betriebssystem nicht trennen kann. Der SafeGuard PortProtector Client versucht zu einem späteren Zeitpunkt, das Gerät zu trennen, und/oder sperrt es nach dem nächsten Neustart.
- **Gewaltsam**: Wenn Sie diese Option wählen, trennt SafeGuard PortProtector das Gerät sofort, unabhängig vom Betriebssystem und jeden Kommunikationskanal zwischen dem Gerät und dem Computer. In sehr seltenen Fällen können dadurch einige Daten, die zum Zeitpunkt der Trennung zu oder von diesem Gerät übertragen wurden, oder das Gerät selbst wegen Datenbeschädigung unbrauchbar werden.

**Hinweis:** Wir empfehlen, die Benutzer in jedem Fall frühzeitig darüber zu unterrichten, dass bestimmte Geräte nicht länger zugelassen sein werden.

**Hinweis:** Bei WiFi-Links wird bei der Zuweisung einer neuen Policy zu einem Client ein vorhandener Link gesperrt und die Verbindung wird erzwungenermaßen getrennt.

#### 3.3.16.1.5 Definieren des Intervalls für die Policy-Aktualisierung

**Hinweis:** Dieser Abschnitt wird auf der Seite *Optionen* nur dann angezeigt, wenn Sie den Policy-Server für die Policy-Verteilung nutzen.

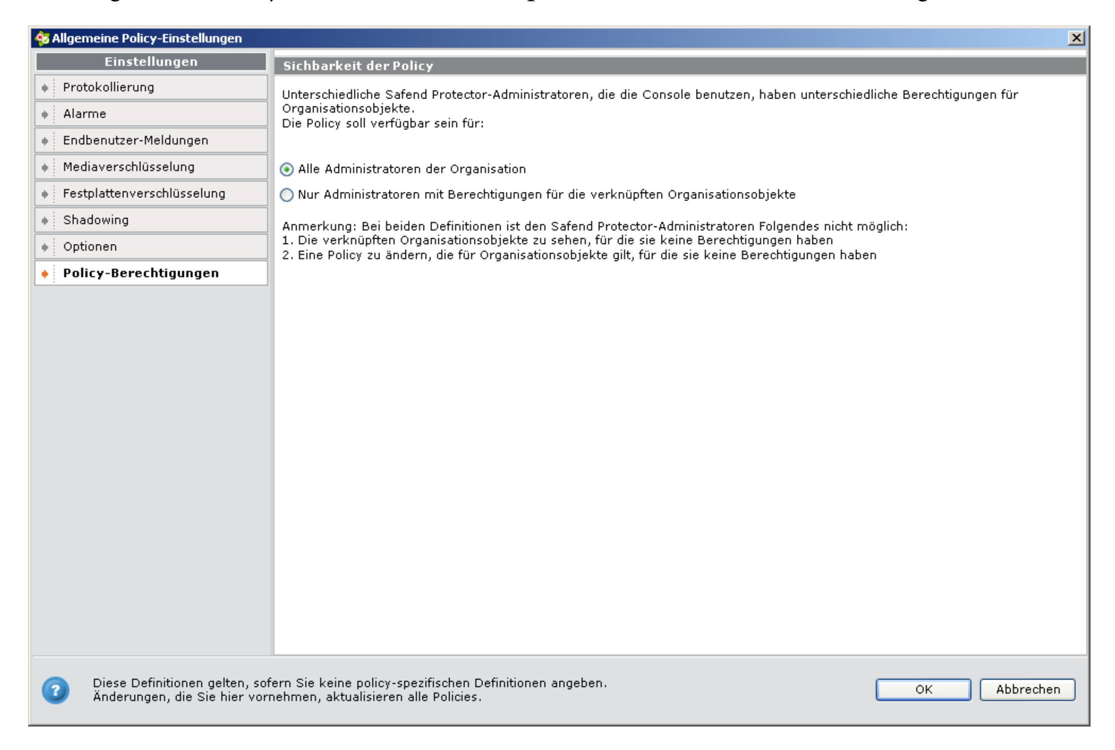
Wenn Policies direkt vom Management Server an die Clients veröffentlicht werden (Verteilungsoption des Policy-Servers), müssen Sie das Intervall festlegen, in dem der Client eine aktualisierte Policy abruft. Legen Sie in diesem Abschnitt das Intervall fest.

## 3.3.17 Schritt 17: Policy-Berechtigungen definieren

**So definieren Sie die Domänenpartitionierung:**

Wählen Sie eine der folgenden Optionen:

- **Alle Administratoren der Organisation:** Um anzugeben, dass alle Administratoren die Policy unabhängig von ihrer Zuordnung sehen können.
- **Nur Administratoren mit Berechtigungen für die verknüpften Organisationsobjekte:** Um anzugeben, dass ein Administrator diese Policy nur sieht, wenn ihre zugehörigen Organisationsobjekte in der Domänenpartition eines Administrators liegen.



### 3.3.17.1 Definieren von Policy-Berechtigungen

**Hinweis:** Die Einstellungen für die Policy-Berechtigung sind nur dann relevant, wenn die Funktion der Domänenpartitionierung aktiviert ist und im Safend Protector-System ein Policy-Server genutzt wird.

Mit Safend Protector Domain Partitioning ist die Partitionierung der Organisationseinheiten und Domänen (auch als *Container* bezeichnet) einer Organisation möglich, so dass darauf nur von den Safend Protector Console-Administratoren zugegriffen werden kann, die für deren Bearbeitung verantwortlich sind. Die Domäne Ihrer Organisation kann gemäß ihrer Organisationsstruktur partitioniert werden, und den einzelnen Domänenpartitionen können dabei verschiedene Safend Protector-Administratoren zugeordnet werden. Eine Beschreibung für die Definition von Domänenpartitionen finden Sie in *Definieren* von Domänenpartitionen.

In Bezug auf Policies bedeutet das, dass Administratoren nur solche Policies ändern können, die mit Organisationsobjekten verknüpft sind, die zu der ihnen zugeteilten Domänenpartition gehören.

Policies, die mit Organisationsobjekten verknüpft sind, die nicht zu der dem Administrator zugewiesenen Domänenpartition gehören, werden im Bereich **Policy mit Organisationsobjekten verknüpfen** des Fensters Policy und in Policy-Abfragen nicht angezeigt und können nicht geändert werden.

Es gibt jedoch eine Ausnahme hinsichtlich einer Policy, die mit **einigen** der Container in der Domäne eines Administrators verknüpft ist, aber **nicht mit anderen**. Das folgende Beispiel beschreibt diese Situation.

**Beispiel:**

Gerhard ist Administrator der Container A, B und C. Das bedeutet, dass sie zu der Domänenpartition gehören, die seiner Rollenberechtigung zugeordnet sind.

Maria ist Administrator der Container A, B und D.

Eine Policy, die mit den Containern A und C verknüpft ist, kann nur von Gerhard modifiziert werden. Maria kann sie nicht modifizieren, weil das bedeuten würde, dass dadurch auch die Policy beeinflusst würde, die zu Container C gilt, der nicht zu ihrer Domänenpartition gehört. Maria kann diese Policy nur im schreibgeschützten Modus sehen. Sie sieht nur die Organisationsobjekte, die mit dieser Policy verknüpft sind und zu ihrer Domänenpartition gehören (Bestandteil der Container A, B und D).

Ein Safend-Administrator kann keine Policies bearbeiten, die mit Organisationsobjekten verknüpft sind, die nicht Bestandteil der ihm zugewiesenen Domänenpartition sind. Er kann auch nicht sehen, welche Organisationsobjekte aus diesen Containern mit der Policy im Bereich **Policy mit Organisationsobjekten verknüpfen** des Fensters Policy verknüpft sind.

Mit Safend Protector haben Sie die Möglichkeit anzugeben, ob ein Administrator Policies, die nicht mit Organisationsobjekten in der ihm zugewiesenen Domänenpartition verknüpft sind, im Modus **Schreibgeschützt** oder **gar nicht** sehen kann. Im schreibgeschützten Modus kann der Administrator die Verknüpfung der Policy mit weiteren Organisationsobjekten ändern, ohne die vorhandenen zu entfernen.

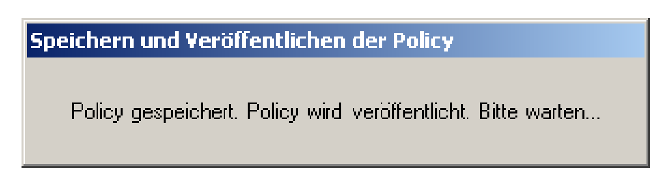
## 3.3.18 Schritt 18: Policy speichern und veröffentlichen

Alle neuen Policies und alle Änderungen an einer Policy müssen gespeichert werden. Eine Policy kann unter ihrem Namen oder mit einem neuen Namen gespeichert werden. (Speichern Sie eine Policy unter einem neuen Namen, wenn es sich um eine neue Policy handelt oder Sie eine Kopie einer vorhandenen Policy speichern möchten.) Beim Speichern einer Policy wird sie auch als GPO in Active Directory oder als Registry-Datei veröffentlicht, wenn Sie eine dieser Methoden für die Policy-Verteilung gewählt haben. (Für weitere Informationen hierzu siehe Übersicht im Kapitel *Verteilen von Policies*.)

### 3.3.18.1 Speichern einer Policy unter ihrem Namen

**So speichern Sie eine vorhandene Policy unter demselben Namen:**

Wählen Sie im Menü *Datei* die Option **Speichern und veröffentlichen**, oder klicken Sie in der Symbolleiste auf das Symbol Speichern und veröffentlichen (). Das folgende Fenster wird angezeigt:



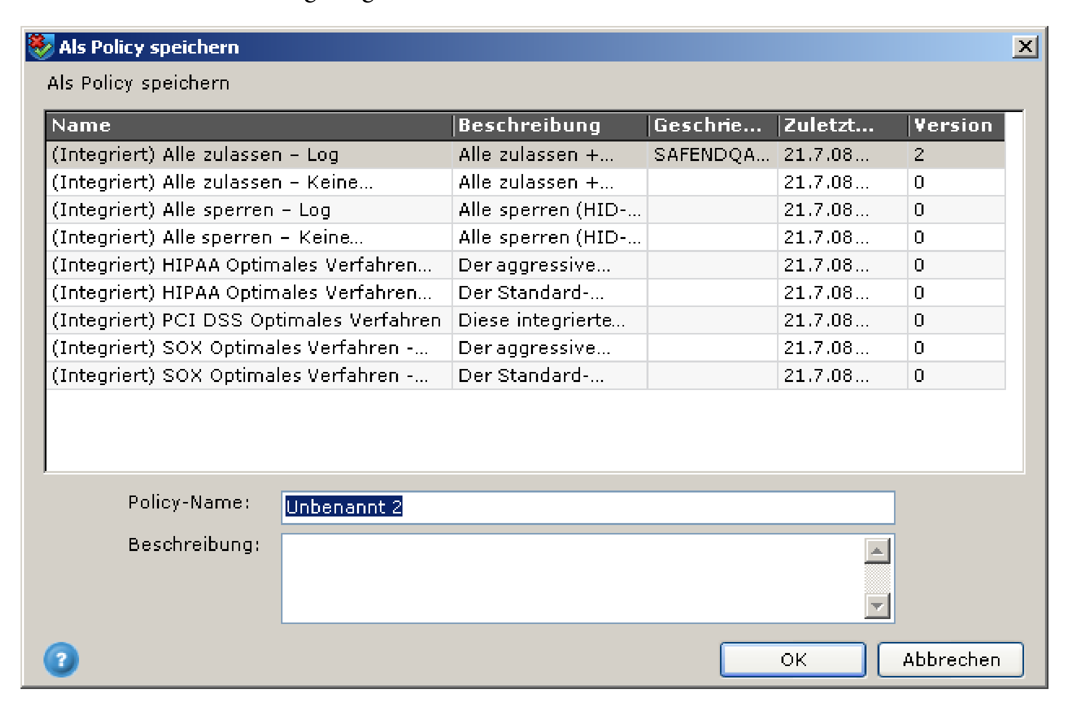

Die Policy wird gespeichert und veröffentlicht.

### 3.3.18.2 Speichern einer Policy unter einem neuen Namen

Sie können eine Policy unter einem neuen Namen mit einer neuen Beschreibung speichern. Dies erfolgt im Fenster *Als Policy speichern*.

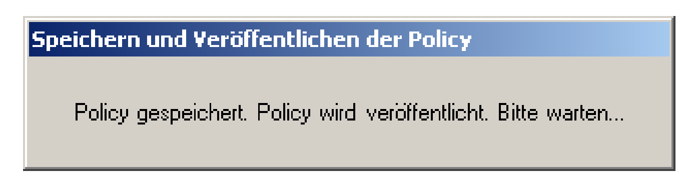
**So öffnen Sie das Fenster Als Policy speichern:**

Wählen Sie im Menü *Datei* die Option **Speichern unter.** Im folgenden Fenster wird eine Liste vorhandener Policies angezeigt:




#### 3.3.18.2.1 Eingeben der Policy-Details

Bearbeiten Sie die Felder *Policy-Name* (erforderlich) und *Beschreibung* (optional), und klicken Sie auf **OK.** Das folgende Fenster wird angezeigt:

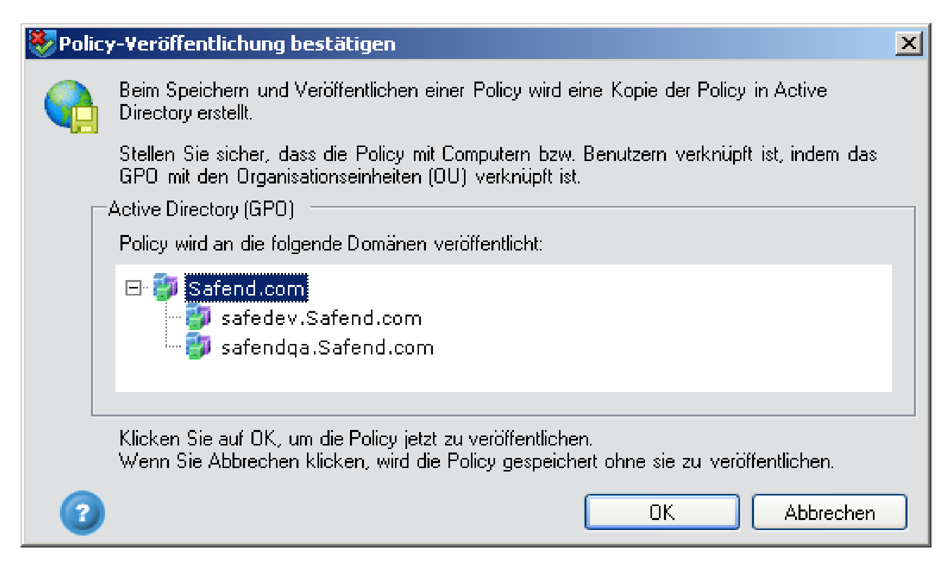



Die Policy wird gespeichert und veröffentlicht.

**Hinweis:** Wenn Sie eine Policy unter einem neuen Namen speichern und Active Directory zur Verteilung von Policies nutzen, hat das neu erstellte GPO keine Verknüpfung zu der erforderlichen Organisationseinheit. Die vorherige Policy gilt, bis Sie das neue GPO mit der Organisationseinheit verknüpfen.

### 3.3.18.3 Bestätigen der Veröffentlichungsdomäne

Wenn Sie beim Veröffentlichen einer Policy zur Aktivierung einer Domänenauswahl aufgefordert werden (siehe Veröffentlichungsmethode im Kapitel *Administration*), wird das Fenster *Policy-Veröffentlichung bestätigen* beim Speichern einer Policy angezeigt:




#### 3.3.18.3.1 Policy-Veröffentlichung bestätigen

Das Fenster zeigt die in Ihrem Organisationsterrain verfügbaren Domänen. Sie können die Policy an die gewünschte Domäne veröffentlichen.

**So bestätigen Sie das Veröffentlichen einer Policy an die ausgewählte Domäne:**

Wählen Sie die Domäne aus, an die die Policy veröffentlicht werden soll, und klicken Sie auf **OK.** Das folgende Fenster wird angezeigt:




Die Policy wird gespeichert und veröffentlicht.

Wenn Sie auf **Abbrechen** klicken, wird die Policy nicht veröffentlicht (d. h. es wird kein GPO bzw. keine Registry-Datei erzeugt), und sie wird lediglich in der Datenbank gespeichert.

**Hinweis:** Wenn Sie Active Directory benutzen, wird beim Speichern und Veröffentlichen einer Policy eine Kopie der Policy (GPO) in Active Directory erstellt. Stellen Sie sicher, dass die Policy mit Computern bzw. Benutzergruppen verknüpft wird, indem Sie das GPO mit der entsprechenden Organisationseinheit verknüpfen.

## 3.4 Freigeben von Geräten und WiFi-Verbindungen

Die Erklärungen in den folgenden Abschnitten beziehen sich auf das Hinzufügen freigegebener Geräte zur *Device Control* White List und das Hinzufügen freigegebener Speichergeräte *Storage Control* White List. Sofern Unterschiede beim Hinzufügen von Speichergeräten und Nicht-Speichergeräten bestehen, wird darauf hingewiesen und eine Erklärung geliefert.

Erläuterungen zum Hinzufügen freigegebener WiFi-Netze finden Sie in Hinzufügen von *WiFi-Verbindungen*.

SafeGuard PortProtector bietet Ihnen drei Berechtigungsstufen:

- **Gerätetypen und Speichertypen:** Mit dieser (oben erläuterten) Option können Sie den Zugriff auf einen Port je nach Typ des daran angeschlossenen Geräts beschränken. Zum Beispiel: Wechselmedien, Netzadapter, HID-Geräte (z. B. eine Maus) oder Bildbearbeitungsgeräte. Die zur Auswahl stehenden Geräte- und Speichertypen sind in SafeGuard PortProtector integriert und stehen auf der oben beschriebenen Registerkarte *General* des Fensters *Device Control* und dies Fensters *Storage Control*.
  Ein Gerätetyp kann **blockiert** (Voreinstellung), **zugelassen** oder **eingeschränkt** werden. Wenn Sie einen Gerätetyp **einschränken**, werden alle Geräte dieses Typs gesperrt, sofern sie nicht gesondert freigegeben werden. Speichergeräte können auch eine **Schreibgeschützt**-Berechtigungen haben.
- **Freigegebene Modelle:** Diese Option bezieht sich auf die Freigabe von Modellen eines Geräts oder Speichergeräts, wie etwa alle HP-Drucker oder alle M-Systems Disk-on-keys.
- **Freigegebene spezifische Geräte:** Diese Option bezieht sich auf die Freigabe spezifischer Geräte bzw. Speichergeräte, von denen jedes eine eindeutige Seriennummer hat, so dass es eigentlich ein spezifisches Gerät ist.

Zum Beispiel: Wenn Sie die Nutzung des Disk-on-Key des CEO freigeben und alle anderen Disk-on-Key-Geräte sperren möchten, müssen Sie den Speichertyp Removable Media auf **Einschränken** setzen und dann die kennzeichnenden Parameter für das USB-Gerät des CEO in einer spezifischen Gerätegruppe eingeben.

Dieser Abschnitt beschreibt, wie freigegebenen Modelle oder spezifische Geräte entweder über die Liste der Geräte, deren Nutzung in Ihrer Organisation von SafeGuard PortAuditor erkannt wurde, mit Hilfe des Assistenten **Freigegebenes Gerät hinzufügen** (siehe *Hinzufügen eines Geräts mit Hilfe des* Assistenten) oder manuell hinzugefügt werden.

Sie können die Berechtigungen für freigegebene Modelle und spezifische Geräte auf der Registerkarte *Ausnahmen* des Fensters *Gerätekontrolle* und des Fensters *Speicherkontrolle* festlegen, die – wie zuvor beschrieben – in die Abschnitte **Freigegebene Modelle** und **Spezifische Geräte** aufgeteilt sind.

Freigegebene Geräte werden der weißen Liste mit den folgenden Schritten hinzugefügt:

- Hinzufügen einer Gerätegruppe
- Hinzufügen von Modellen und spezifischen Geräten zur Gerätegruppe, entweder mit Hilfe des Assistenten oder manuell
- Festlegen der Gruppenberechtigungen
- Hinzufügen weiterer Gruppeneinstellungen (wie Log- und Alarmeinstellungen)
- Speichern der Policy

### 3.4.1 Hinzufügen von Gerätegruppen

Freigegebene Modelle und spezifische Geräte werden in Gruppen angeordnet, damit Sie zusammengehörige Geräte mit denselben Berechtigungen leichter verwalten können (z. B. alle Geräte, die von der Marketing-Gruppe benutzt werden). Bevor Sie Geräte hinzufügen können, müssen Sie Gerätegruppen festlegen. Je nach Bedarf können Sie Gruppen von Modellen oder spezifischen Geräten definieren.

**So fügen Sie eine neue Gruppe hinzu:**

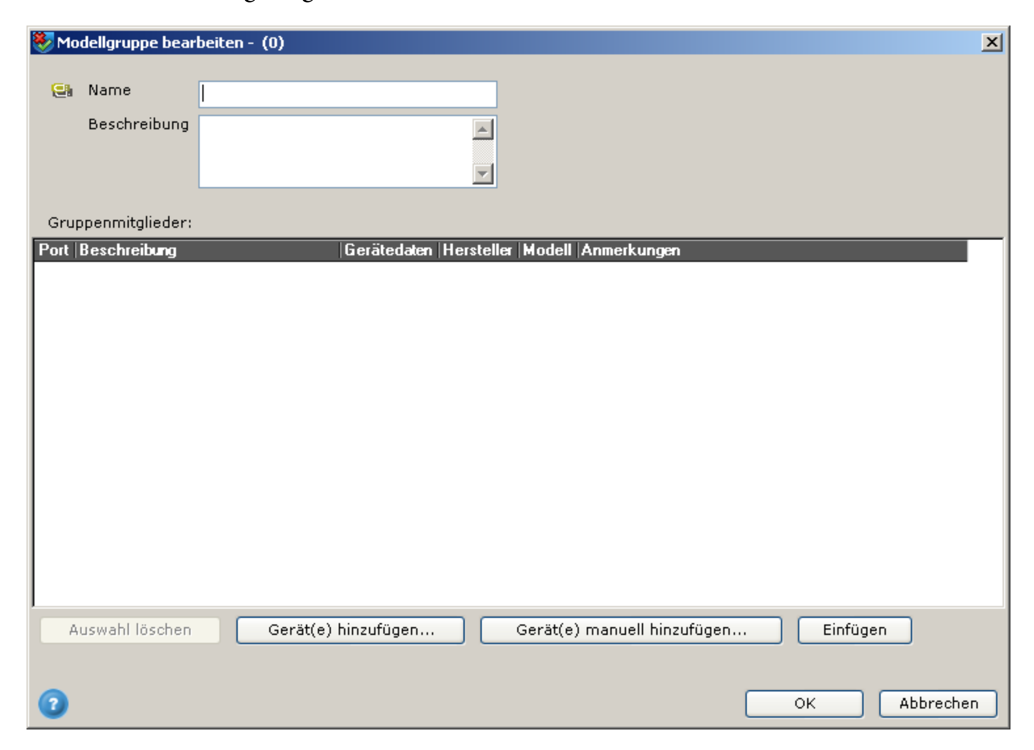
**Hinweis:** Der untere Abschnitt der Registerkarte Speicherkontrolle Ausnahmen heißt Freigegebene spezifische Geräte/Medien.

1 Klicken Sie im Bereich **Freigegebene Modelle** oder **Freigegebene spezifische Geräte** auf die Schaltfläche **Hinzufügen** . Ein Menü wird angezeigt. Wenn Sie sich im Abschnitt **Freigegebene spezifische Geräte/Medien** der Registerkarte **Speicherkontrolle** *Ausnahmen* befinden, wird ein Untermenü angezeigt.

ODER

Klicken Sie mit der rechten Maustaste im Abschnitt **Freigegebene Modelle** oder **Freigegebene spezifische Geräte** auf die Registerkarte *Weiße Liste*. Ein Menü wird angezeigt.

2 Klicken Sie auf **Neue Gruppe** im Menü bei **Freigegebene Modelle.** Das Fenster *Modellgruppe bearbeiten* wird angezeigt:




### 3.4.1.1 Hinzufügen einer Gruppe

Für jedes von Ihnen hinzugefügte Gerät wird in diesem Fenster eine Beschreibung des Geräts, der Gerätehersteller, das Gerätemodell und die eindeutige Geräte-ID (bei einer Gruppe Freigegebene spezifische Geräte) und ggf. Anmerkungen angezeigt.

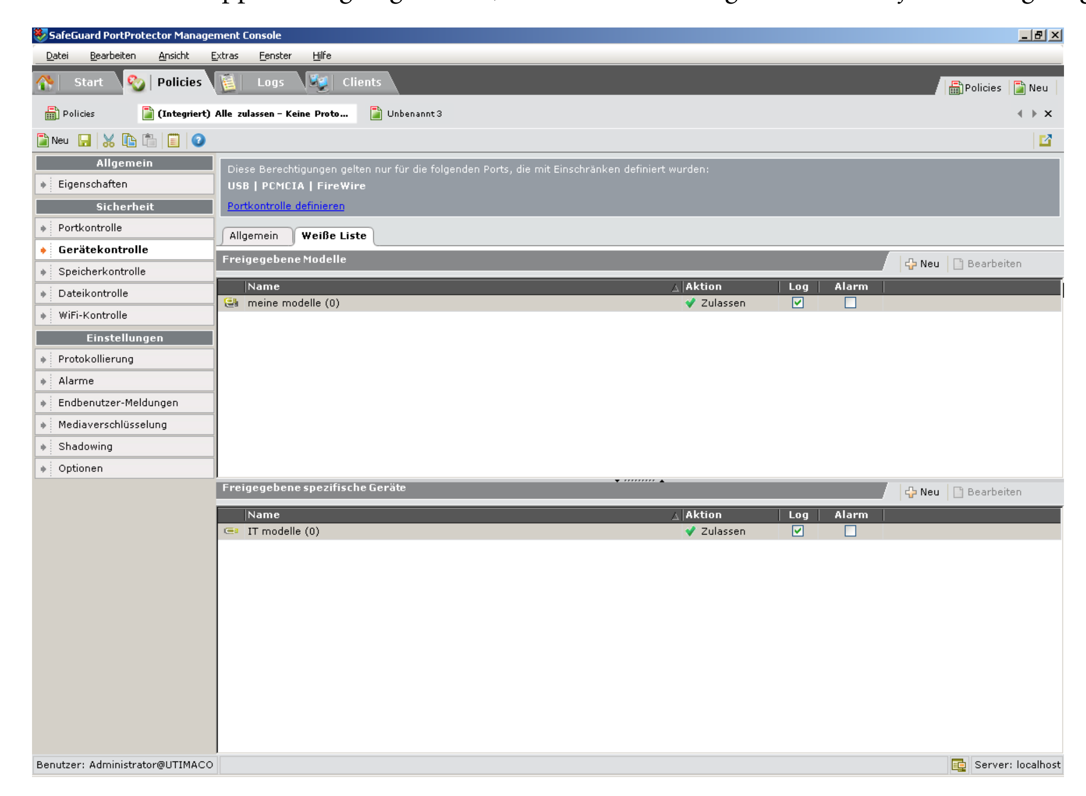
1 Mit den Schaltflächen unterhalb der Geräteliste können Sie Geräte löschen oder Geräte entweder mit Hilfe des Assistenten für das Hinzufügen freigegebener Geräte (siehe *Hinzufügen eines Geräts mit Hilfe des Assistenten*) oder manuell (siehe *Manuelles Hinzufügen eines Geräts*) hinzufügen. Alternativ klicken Sie mit der rechten Maustaste auf den leeren Bereich unter **Gruppenmitglieder** und wählen dann **Gerät(e) hinzufügen Assistent** oder **Gerät(e) manuell hinzufügen.**
Geben Sie in diesem Fenster bei **Name** (erforderlich) den gewünschten Gruppennamen und bei **Beschreibung** (optional) eine Beschreibung ein.

2 Fügen Sie Geräte zur Gruppe wie nachfolgend beschrieben hinzu. Sie können auch zu einem späteren Zeitpunkt Geräte zu dieser Gruppe hinzufügen.

3 Wenn Sie fertig sind, klicken Sie auf **OK.**

Sie können auch eine Gruppe aus der Zwischenablage **einfügen.** Hierfür benutzen Sie die Symbolleistenschaltfläche **Einfügen** oder die Option **Einfügen** im Menü *Bearbeiten.*

Sobald eine Gruppe hinzugefügt wurde, wird sie auf der Registerkarte *Weiße Liste* angezeigt:




In der obigen Abbildung sind zwei Gruppen zu sehen. Die Gruppen sind automatisch als zugelassen (✔) markiert.

## 3.4.2 Bearbeiten einer Gerätegruppe

Nachdem eine Gruppe angelegt wurde, kann sie modifiziert werden.

**So bearbeiten Sie eine Gerätegruppe:**

Doppelklicken Sie auf der Registerkarte *Weiße Liste* auf die gewünschte Gruppe.

ODER

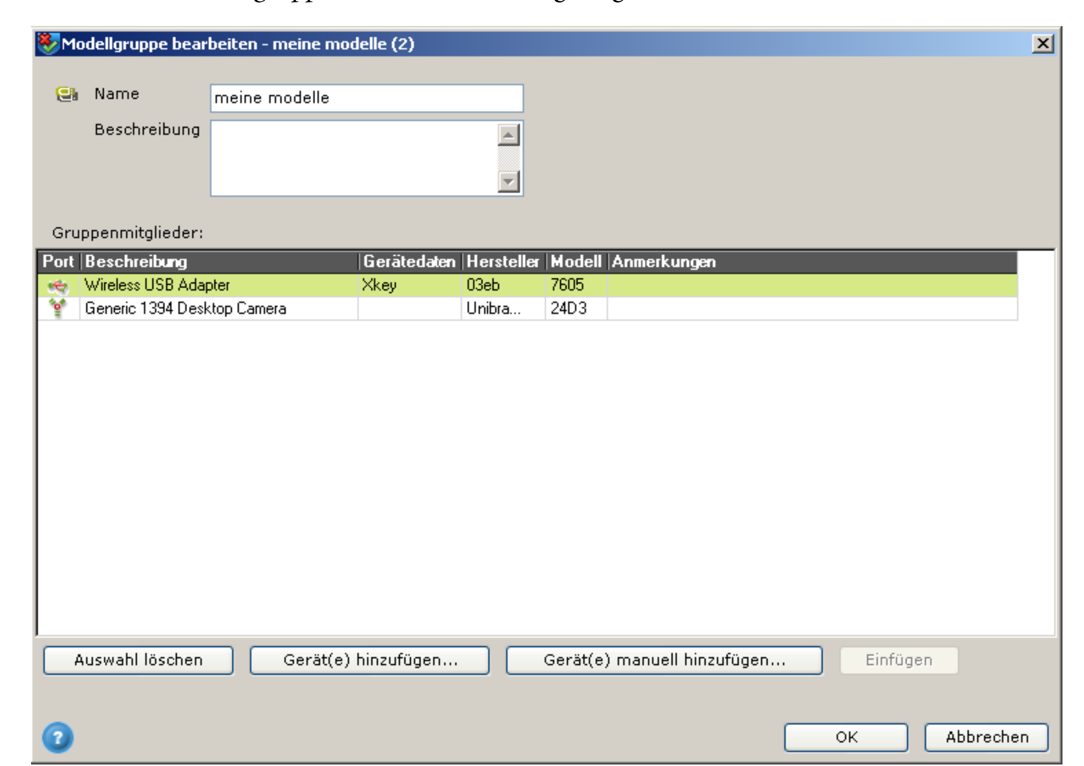
1 Wählen Sie die zu bearbeitende Gruppe aus.

2 Klicken Sie auf die Schaltfläche **Gruppe bearbeiten** ( ).

ODER

Klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe und klicken Sie dann im Menü auf **Bearbeiten**.

Das Fenster *Modellgruppe bearbeiten* wird angezeigt:




### 3.4.2.1 Bearbeiten einer Gruppe

Falls Sie dieser Gruppe bereits Geräte hinzugefügt haben, werden in dem Fenster auch die zur Gruppe gehörigen Geräte angezeigt. Für jedes Gerät wird eine Beschreibung des Geräts, der Gerätehersteller, das Gerätemodell und die eindeutige Geräte-ID (bei einer Gruppe freigegebener spezifische Geräte) und ggf. Anmerkungen angezeigt.

Mit den Schaltflächen unterhalb der Geräteliste können Sie Geräte löschen oder Geräte entweder mit Hilfe des Assistenten für das Hinzufügen freigegebener Geräte (siehe *Hinzufügen eines Geräts mit Hilfe des Assistenten*) oder manuell (siehe *Manuelles Hinzufügen eines Geräts*) hinzufügen.

Die folgenden Bearbeitungsoptionen sind verfügbar:

- Hinzufügen von Geräten
- Ändern von Gerätedaten
- Löschen von Geräten
- Kopieren von Geräten in eine andere Gruppe oder Einfügen aus einer anderen Gruppe
- Ändern von Gruppen-**Name** und **Beschreibung**.

### 3.4.3 Hinzufügen von Geräten

Geräte können vorhandenen Gruppen oder neuen Gruppen hinzugefügt werden.

**So fügen Sie ein Gerät zu einer vorhandenen Gruppe hinzu:**

Klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe und wählen Sie **Zu Gruppe hinzufügen.** Um ein Gerät mit Hilfe des Assistenten **Freigegebenes Gerät hinzufügen** hinzuzufügen, klicken Sie auf **Über Assistent hinzufügen** und folgen Sie den Anleitungen in *Hinzufügen eines Geräts mit Hilfe des* Assistenten. Um ein Gerät manuell hinzuzufügen, klicken Sie auf **Manuell hinzufügen** und folgen Sie den Anleitungen in *Manuelles Hinzufügen eines Geräts*.

Eine weitere Möglichkeit, Geräte zu einer Gruppe hinzuzufügen, haben Sie im Fenster *Gruppe bearbeiten*:

1 Öffnen Sie das Fenster Edit Group auf einem der in *Bearbeiten einer Gerätegruppe* beschriebenen Wege.

2 Um ein Gerät mit Hilfe des Assistenten **Freigegebenes Gerät hinzufügen** hinzuzufügen, klicken Sie auf **Geräte(e) hinzufügen** und fahren mit dem nächsten Abschnitt – *Hinzufügen eines Geräts mit Hilfe des Assistenten* – fort.
Um ein Gerät manuell hinzuzufügen, klicken Sie auf **Geräte(e) manuell hinzufügen** und fahren Sie mit *Manuelles Hinzufügen eines Geräts* fort.
Wenn Sie USB-Gerätedaten aus einem Log (siehe *Kopieren von USB-Geräten oder CD/DVD-Mediadaten* im Kapitel*, Anzeigen von Logs*) kopiert haben, können Sie auch mit der rechten Maustaste auf den leeren Bereich von im Fenster *Gruppe bearbeiten* klicken und **Einfügen** wählen, um die USB-Gerätedaten in eine Gruppe zu kopieren (vergewissern Sie sich, dass Sie keine Speichergerätedaten in eine Gruppe von Nicht-Speichergeräten – oder umgekehrt – kopieren).

Dieselben Schritte können Sie auch beim Öffnen einer neuen Gruppe verwenden, um Geräte hinzuzufügen.

**Hinweis:** Wenn Sie ein Gerät hinzufügen, das bereits zu einer anderen Gerätegruppe in dieser Policy gehört und die Berechtigungen der Gruppen unterschiedlich sind, gelten die mit mehr Berechtigungen: **Zulassen** gibt die höchste Berechtigung, **Verschlüsseln** verleiht weniger Berechtigung (ist wie **Zulassen** bei Verschlüsselung) und **Schreibgeschützt** vergibt die geringste Berechtigung.

Zum Beispiel: Wenn die Gruppe Freigegebene Modelle, die ein Speichergerät enthält, auf **Zulassen** gesetzt ist und das spezifische Gerät auf **Schreibgeschützt** gesetzt ist, gilt die Berechtigung **Zulassen.** Log- and Alarmeinstellungen werden ebenfalls von der Definition mit den meisten Berechtigungen übernommen.

Falls ein Gerät zu mehreren Gruppen gehört, und diese Gruppen dieselben Berechtigungen haben, wird SafeGuard PortProtector die Gruppen willkürlich auswählen. Wenn die Gruppen nicht dieselben Log- und Alarmeinstellungen haben, ist es nicht vorhersehbar, welche Einstellungen angewendet werden.

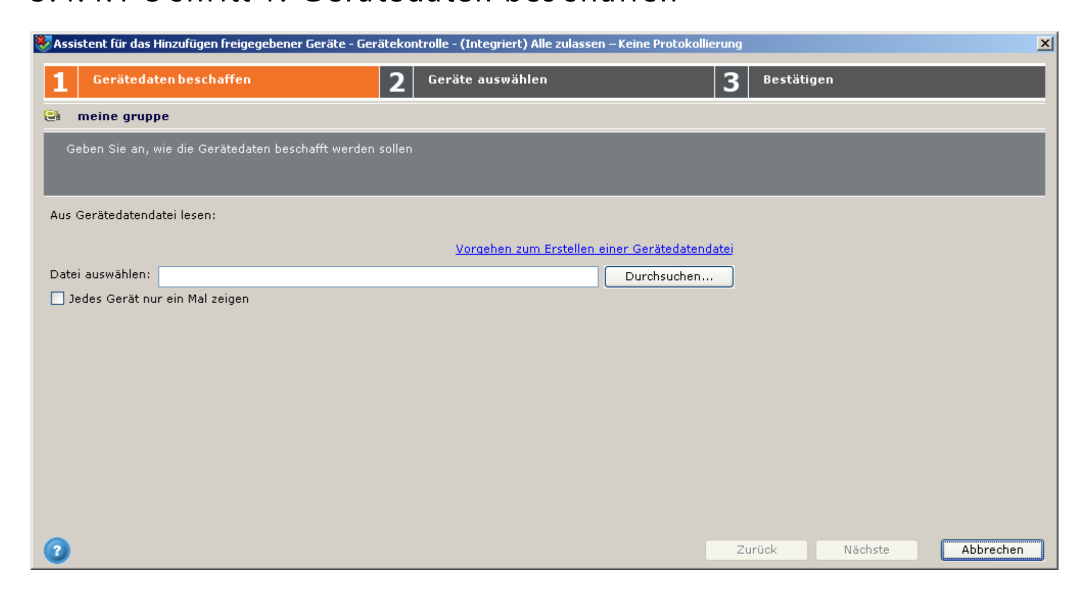
## 3.4.4 Hinzufügen eines Geräts mit Hilfe des Assistenten

Sobald Sie Gerätegruppen definiert haben, steht ein einfacher Assistent **Freigegebenes Gerät hinzufügen** zur Verfügung. Dieser leitet Sie durch die Schritte beim Hinzufügen freigegebener Geräte aus einer Liste der zuvor von SafeGuard PortAuditor auf den Computern in Ihrem Netz erkannten Geräten. Sie können Geräte auch manuell hinzufügen (siehe auch *Manuelles Hinzufügen eines Geräts*). Der Assistent wird geöffnet, wenn Sie auf **Gerät(e) hinzufügen** im Fenster *Gruppe bearbeiten* klicken oder **Über Assistent hinzufügen** im Kontextmenü auswählen, wie in *Hinzufügen von Geräten* erläutert.

Der Assistent beinhaltet drei Schritte:

- Schritt 1: Gerätedaten beschaffen
- Schritt 2: Geräte auswählen
- Schritt 3: Bestätigen

### 3.4.4.1 Schritt 1: Gerätedaten beschaffen



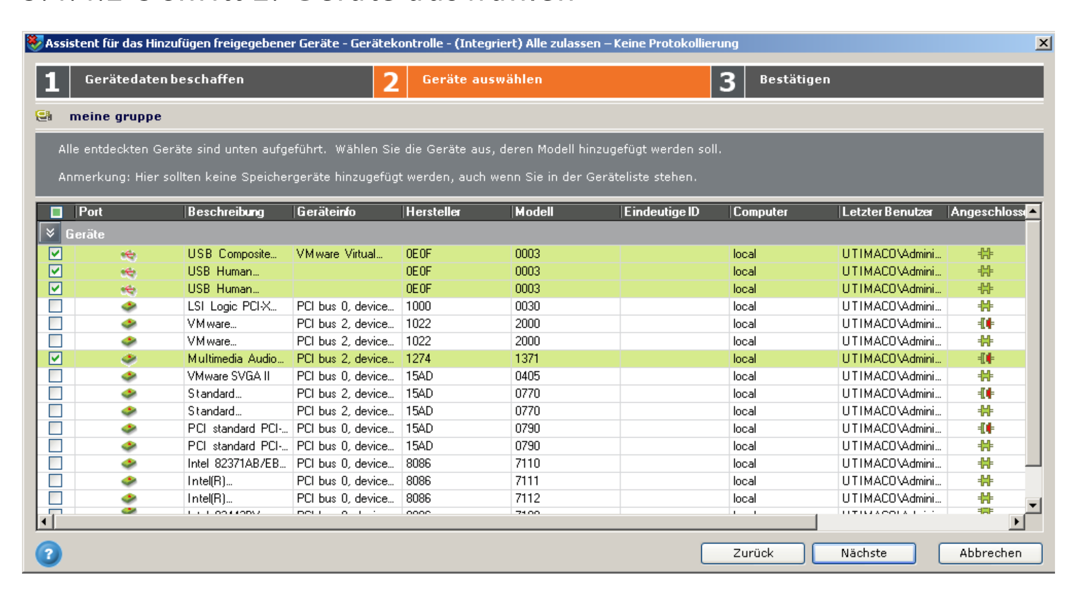

#### 3.4.4.1.1 Beschaffen von Gerätedaten

In diesem Schritt können Sie die Datei angeben, aus der die Informationen über die Geräte entnommen werden, die der Gruppe hinzugefügt werden sollen. Das heißt, Sie können den Speicherort der SafeGuard PortAuditor.XML-Datei angeben, in der die benötigten Gerätedaten enthalten sind. Nachdem Sie die gewünschte Datei über **Browse** ausgewählt haben, klicken Sie auf **Nächste**, um mit Schritt 2 fortzufahren.

##### 3.4.4.1.1.1 Erstellen einer Gerätedatendatei

Um eine Datei zu erstellen, in der die Informationen über die freizugebenden Geräte enthalten sind, verwenden Sie SafeGuard PortAuditor zum Scannen der gewünschten Computer. SafeGuard PortAuditor scannt die ausgewählten Computer und erstellt einen Bericht über alle Geräte und WiFi-Netze, die derzeit oder vorher an diesen Computern angeschlossen sind bzw. waren. Die Prüfergebnisse werden in einer XML-Datei gespeichert. Mehr Informationen zu SafeGuard PortAuditor finden Sie im *SafeGuard PortAuditor 3.2 Benutzerhandbuch*.

### 3.4.4.2 Schritt 2: Geräte auswählen




#### 3.4.4.2.1 Auswählen von Geräten

Schritt 2 zeigt eine Tabelle der Geräte an, die auf den Endpunkten in Ihrem Netz erkannt wurden, und ermöglicht Ihnen die Auswahl der Geräte, die der Gerätegruppe hinzugefügt werden sollen. Die Tabelle ist in Kategorien unterteilt, die davon abhängen, ob Sie Geräte in eine Gruppe freigegebener Modelle oder in eine Gruppe spezifischer Geräte hinzufügen, und ob Sie Speichergeräte oder Nicht-Speichergeräte hinzufügen.

Neben den auswählbaren Geräten steht ein Kontrollkästchen, das Sie markieren müssen, um das Gerätemodell bzw. das spezifische Gerät freizugeben. Geräte, die bereits zur aktuellen Gruppe gehören, sind grau markiert. Das Kontrollkästchen daneben ist bereits markiert.

**Hinweis:** Sie können der weißen Liste in *Gerätekontrolle* keine Speichergeräte hinzufügen.

**Hinweis:** Geräte oder Speichergeräte ohne eindeutige ID können einer Gruppe Spezifische Geräte nicht hinzugefügt werden.

Gelegentlich kann es vorkommen, dass ein Gerät von SafeGuard PortAuditor nicht als Speichergerät gekennzeichnet wurde. Das kann z. B. dann vorkommen, wenn eine Geräteklasse vom Hersteller nicht integriert wurde. In diesem Fall können Sie das Gerät zur weißen Liste der Speichergeräte in Ihrer Policy eintragen, wenn Sie wissen, dass es tatsächlich ein Speichergerät ist.

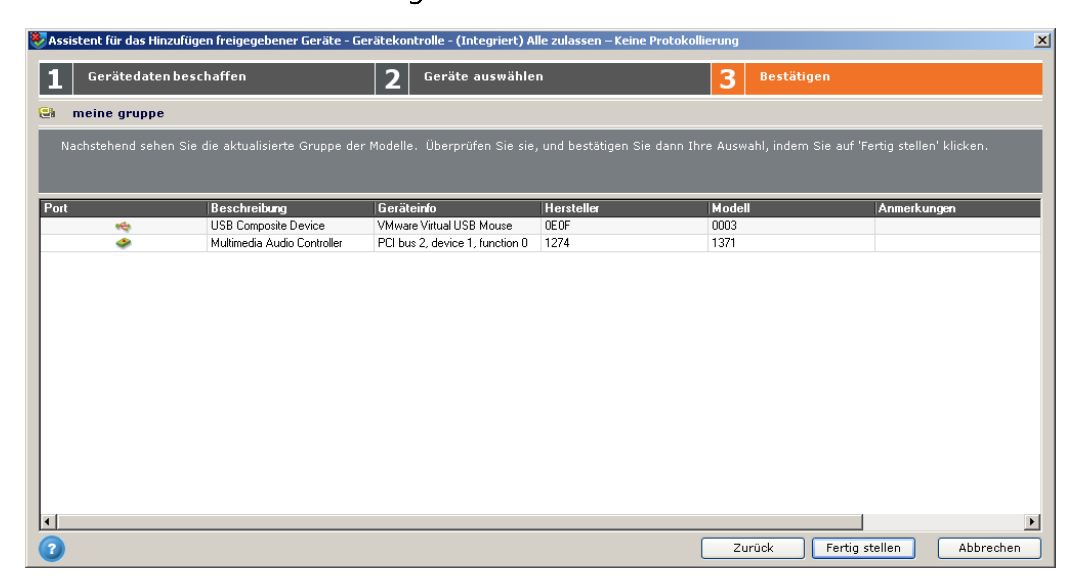
Sorgen Sie dafür, dass der Ausnahmenliste bei *Gerätekontrolle* keine Speichergeräte und einer Ausnahmenliste bei *Speicherkontrolle* keine Nicht-Speichergeräte hinzugefügt werden, weil sie durch den SafeGuard PortProtector Client ignoriert würden.

**Hinweis:** Wenn Sie ein Gerät hinzufügen, das bereits zu einer anderen Gerätegruppe in dieser Policy gehört und die Berechtigungen der Gruppen unterschiedlich sind, gelten die mit mehr Berechtigungen. Zum Beispiel: Wenn die Gruppe Freigegebene Modelle, die ein Speichergerät enthält, auf **Zugelassen** gesetzt ist und das spezifische Gerät auf **Schreibgeschützt** gesetzt ist, gilt die Berechtigung **Zugelassen.** Log- and Alarmeinstellungen werden ebenfalls von der Definition mit den meisten Berechtigungen übernommen.

Falls ein Gerät zu mehreren Gruppen gehört, und diese Gruppen dieselben Berechtigungen haben, wird SafeGuard PortProtector die Gruppen willkürlich auswählen. Wenn die Gruppen nicht dieselben Log- und Alarmeinstellungen haben, ist es nicht vorhersehbar, welche Einstellungen angewendet werden.

Sobald Sie die der Gruppe hinzuzufügenden Geräte ausgewählt haben, klicken Sie auf **Nächste**, um mit Schritt 3 fortzufahren.

### 3.4.4.3 Schritt 3: Bestätigen




#### 3.4.4.3.1 Bestätigen der Auswahl

Hier bestätigen Sie Ihre Auswahl und überprüfen die Gruppe mit den neu hinzugefügten Geräten.

Zur Bestätigung der Auswahl klicken Sie auf **Fertig stellen**. Oder klicken Sie auf **Zurück**, um zum vorherigen Stadium zurückzukehren.

## 3.4.5 Manuelles Hinzufügen eines Geräts

Sie möchten vielleicht Geräte manuell (nicht über den Assistenten Add Approved Device) hinzufügen, z. B. wenn Geräte nicht an einen Endpunkt in Ihrer Organisation angeschlossen waren und deshalb nicht in den Prüfergebnissen von SafeGuard PortAuditor erscheinen. Je nachdem, ob Sie ein freigegebenes Modell oder ein spezifisches Gerät hinzufügen, wird das Fenster *Gerätemodell hinzufügen* oder *Spezifisches Gerät hinzufügen* angezeigt, wenn Sie auf **Geräte(e) manuell hinzufügen** im Fenster *Gruppe bearbeiten* klicken oder **Manuell hinzufügen** im Kontextmenü (siehe "Hinzufügen von Geräten" weiter oben) auswählen.

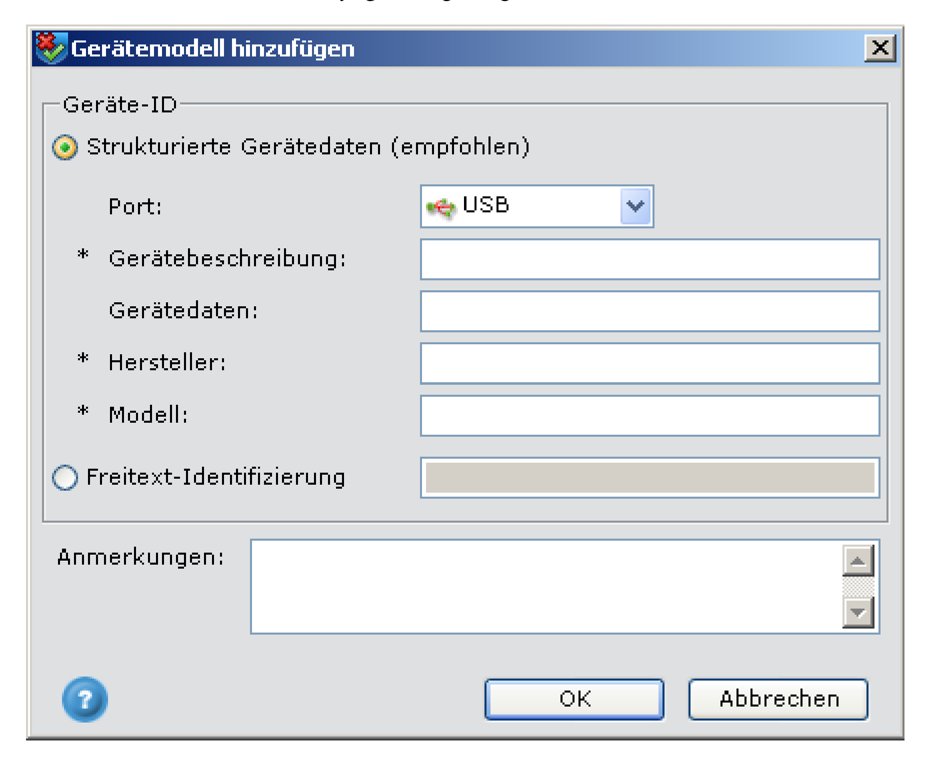
Die folgenden Anleitungen gelten sowohl für das Hinzufügen von Speichergeräten (in *Speicherkontrolle*) als auch für das Hinzufügen von Nicht-Speichergeräten (in *Gerätekontrolle*).

**Hinweis:** Wenn Sie ein Gerät hinzufügen, das bereits zu einer anderen Gerätegruppe in dieser Policy gehört und die Berechtigungen der Gruppen unterschiedlich sind, gelten die mit mehr Berechtigungen. Zum Beispiel: Wenn die Gruppe Freigegebene Modelle, die ein Speichergerät enthält, auf **Zugelassen** gesetzt ist und das spezifische Gerät auf **Schreibgeschützt** gesetzt ist, gilt die Berechtigung **Zugelassen.** Log- and Alarmeinstellungen werden ebenfalls von der Definition mit den meisten Berechtigungen übernommen.

Falls ein Gerät zu mehreren Gruppen gehört, und diese Gruppen dieselben Berechtigungen haben, wird SafeGuard PortProtector die Gruppen willkürlich auswählen. Wenn die Gruppen nicht dieselben Log- und Alarmeinstellungen haben, ist es nicht vorhersehbar, welche Einstellungen angewendet werden.

### 3.4.5.1 Hinzufügen eines freigegebenen Modells

Wenn Sie ein Gerätemodell zu einer Gruppe freigegebener Modelle hinzufügen, wird das Fenster *Gerätemodell hinzufügen* angezeigt:




Zur Identifizierung des Geräts stehen zwei Optionen zur Verfügung:

- **Strukturierte Gerätedaten:** Hiermit können Sie in Feldern Informationen zum Gerät eingeben, anhand derer SafeGuard PortProtector es identifizieren kann, wie im nächsten Abschnitt beschrieben. Dies ist die empfohlene Option. Sie ist für die meisten Geräte geeignet, weil sie auf gängigen Konventionen für Gerätedaten beruht, die von den meisten Hardwareherstellern verwendet werden.
- **Freitext-Identifizierung:** Hiermit können Sie freien Text für Informationen zum Gerät eingeben, anhand derer SafeGuard PortProtector es identifizieren kann. Verwenden Sie diese Option nur, wenn Sie die Felder bei der Option **Strukturierte Gerätedaten** in den SafeGuard PortProtector-Logs nicht sehen können.

#### 3.4.5.1.1 Eingeben der Gerätemodelldaten

Geben Sie im Fenster *Gerätemodell hinzufügen* die Gerätemodelldaten wie folgt ein:

**So fügen Sie ein Gerätemodell hinzu:**

1 Wählen Sie die Methode zur Geräteidentifizierung: Structured Information (empfohlen) oder Freitext-Identifizierung, wie oben beschrieben.

2 Wenn Sie die strukturierte Geräteidentifizierung gewählt haben:

- Wählen Sie im Menü **Port** den Porttyp aus.

Hinweis: Für FireWire- und PCMCIA-Ports stehen mehrere Optionen zur Verfügung. Wenn Sie sich bezüglich der richtigen Option nicht sicher sind, sehen Sie im Windows-Gerätemanager oder in den SafeGuard PortAuditor-Scanergebnissen nach.

3 Tragen Sie die erforderlichen Daten in den folgenden Feldern ein:

- Gerätebeschreibung, erforderlich
- Gerätedaten, optional
- Hersteller (Hersteller-ID) erforderlich
- Modell (Produkt-ID), erforderlich.

**Hinweis:** Die Hersteller-ID (VID) und Produkt-ID (PID) können Sie in den SafeGuard PortAuditor-Scanergebnissen, auf einem Aufkleber auf dem Produkt selbst, oder im Windows-Gerätemanager finden.

Verwenden Sie die Option *Freitext-Identifizierung* nur, wenn die Felder Hersteller und Modell in dem Log für das in die Ausnahmen aufzunehmende Gerät leer sind. Im Feld *Freitext-Identifizierung* können Sie die Hardware-ID des Geräts eingeben.

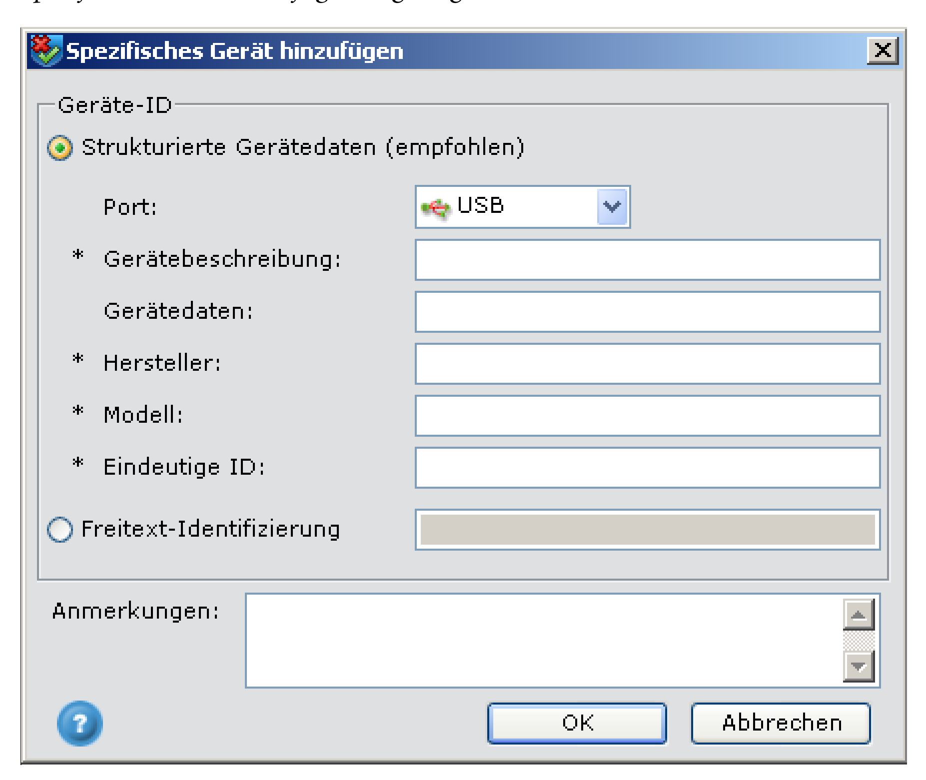
**Hinweis:** Die Hardware-ID finden Sie im **Gerätemanager** – Registerkarte **Details**.

4 Geben Sie **Anmerkungen** ein – optional.

5 Überprüfen Sie gewissenhaft, ob Sie in allen Feldern die richtigen Daten eingegeben haben, und klicken Sie auf **OK**.

### 3.4.5.2 Hinzufügen eines spezifischen Geräts

Wenn Sie ein Gerät zu einer Gruppe freigegebener Modelle hinzufügen, wird das Fenster *Spezifisches Gerät hinzufügen* angezeigt:




Das Fenster ist etwas anders als das Fenster *Gerätemodell hinzufügen*, da es ein weiteres Pflichtfeld **Eindeutige ID** enthält.

#### 3.4.5.2.1 Eingeben der Daten für das spezifische Gerät

Geben Sie im Fenster *Add Distinct Device* die Gerätemodelldaten wie folgt ein:

**So fügen Sie ein spezifisches Gerät hinzu:**

1 Wählen Sie die Methode zur Geräteidentifizierung: Strukturierte Gerätedaten (empfohlen) oder Freitext-Identifizierung, wie oben beschrieben.

2 Wenn Sie die strukturierte Geräteidentifizierung gewählt haben:

- Wählen Sie im Menü **Port** den Porttyp aus.

**Hinweis:** Für FireWire- und PCMCIA-Ports stehen mehrere Optionen zur Verfügung. Wenn Sie sich bezüglich der richtigen Option nicht sicher sind, sehen Sie im Windows-Gerätemanager oder in den SafeGuard PortAuditor-Scanergebnissen nach.

- Tragen Sie die erforderlichen Daten in den folgenden Feldern ein:
- Gerätebeschreibung, erforderlich
- Gerätedaten, optional
- Hersteller (Hersteller-ID) erforderlich
- Modell (Produkt-ID), erforderlich.

**Hinweis:** Die Hersteller-ID (VID) und Produkt-ID (PID) können Sie in den SafeGuard PortAuditor-Scanergebnissen, auf einem Aufkleber auf dem Produkt selbst, oder im Windows-Gerätemanager finden.

Verwenden Sie die Option *Freitext-Identifizierung* nur, wenn die Felder Hersteller und Modell in dem Log für das in die Ausnahmen aufzunehmende Gerät leer sind. Im Feld *Freitext-Identifizierung* können Sie die Hardware-ID des Geräts eingeben.

### 3.4.6 Weitere Einstellungen für Gerätegruppen

Nachdem Sie die gewünschten Geräte zu einer Gruppe hinzugefügt haben, müssen Sie noch einige Einstellungen definieren:

- Log- and Alarmeinstellungen
- Aktion (nur Speichergeräten)
- Gruppenberechtigungen, spezielle Einstellungen für Disk-on-key Smart-Funktionalität (nur Speichergeräte).

**So definieren Sie Log- and Alarmeinstellungen:**

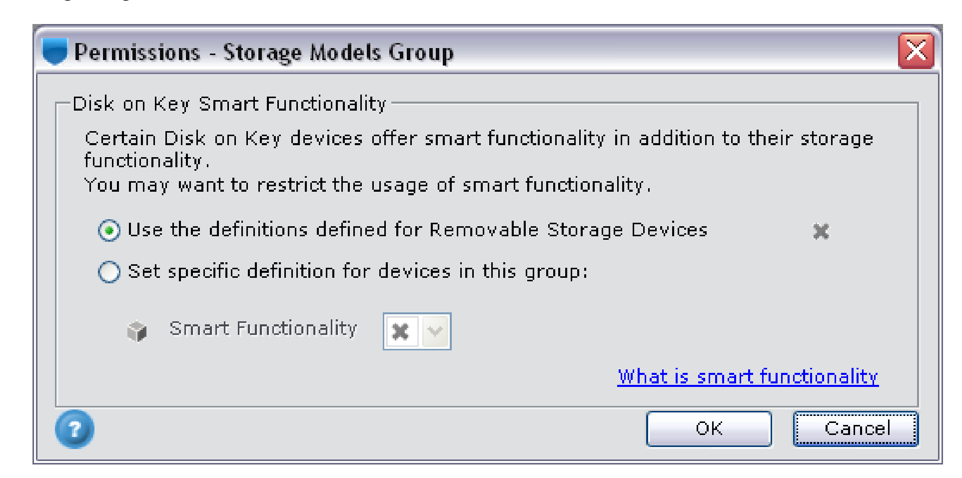
Markieren Sie bei Bedarf für jede Gruppe die Kontrollkästchen *Log* und *Alarm*.

So legen Sie Gruppendefinitionen fest (nur Speicher):

Wählen Sie im Menü *Action* aus, ob die Berechtigung der Gruppe **Zulassen** ( ), **Verschlüsseln** ( ) oder **Schreibgeschützt** ( ) sein soll (Nicht-Speichergeräte sind automatisch auf **Zulassen** gesetzt und können nicht konfiguriert werden)

**So definieren Sie spezielle Einstellungen für Disk-on-key Smart-Funktionalität (nur Speicher):**

Klicken Sie auf die Schaltfläche **Berechtigungen** der Gruppe. Das folgende Fenster wird angezeigt:




#### 3.4.6.1 Berechtigungen für Speichergerätegruppen

Sie können bei Bedarf gruppenspezifische Definitionen für Disk-on-Key Smart-Funktionalität festlegen. Diese Definitionen überschreiben dann die Einstellungen für die Smart-Funktionalität, die Sie auf der Registerkarte *Allgemein* festgelegt haben.

Klicken Sie auf die erste Optionsschaltfläche, wenn Sie die Definitionen nutzen möchten, die Sie auf der Registerkarte *Speichergeräte – Allgemein* festgelegt haben.

Wenn Sie spezifische Definitionen für die Geräte in dieser Gruppe festlegen möchten, klicken Sie auf die zweite Optionsschaltfläche. Wählen Sie dann die gewünschte Berechtigung aus der Dropdown-Liste **Smart-Funktionalität** aus (eine Erklärung der Smart-Funktionalität finden Sie in *Festlegen der Berechtigungen für Wechselspeicher*).

## 3.4.7 Hinzufügen von WiFi-Verbindungen

WiFi-Links werden der weißen Liste bei *WiFi Control* in ähnlicher Weise hinzugefügt wie bei Geräten: Hinzufügen von WiFi-Gruppen, dann Hinzufügen freigegebener Links zu dieser Gruppe mit Hilfe des Assistenten **Freigegebene WiFi hinzufügen** oder manuell.

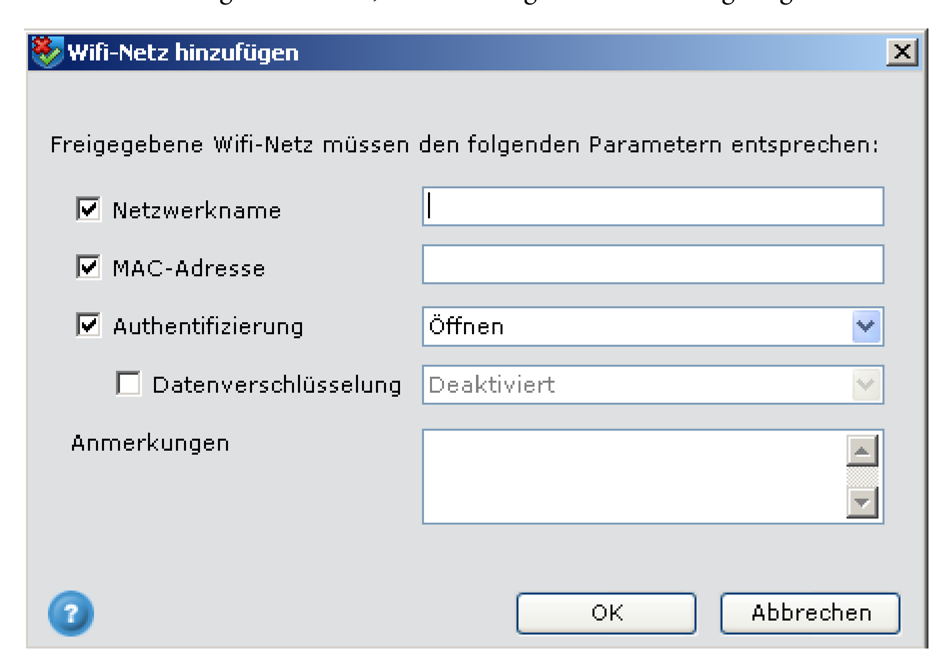
So fügen Sie freigegebene WiFi-Links hinzu:

Außer beim manuellen Hinzufügen von WiFi-Links folgen Sie einfach den Anleitungen für das Hinzufügen von Geräten wie folgt:

- *Hinzufügen von Gerätegruppen*
- *Hinzufügen von Geräten*
- *Hinzufügen eines Geräts mit Hilfe des Assistenten*
- *Weitere Einstellungen für Gerätegruppen*

### 3.4.7.1 Manuelles Hinzufügen von WiFi-Links

Sie können WiFi-Links, die nicht von SafeGuard PortAuditor erkannt wurden und daher nicht mit Hilfe des Assistenten hinzugefügt werden können, manuell hinzufügen. Wenn Sie ein Netz manuell hinzufügen möchten, wird das folgende Fenster angezeigt:



#### 3.4.7.1.1 Eingeben der WiFi-Netzwerkdaten

In diesem Fenster definieren Sie Parameter, denen ein Netzwerk entsprechen muss, um für eine Verbindung freigegeben zu werden. Sie können ein Netzwerk anhand seines Namens, seiner MAC-Adresse oder seines Authentifizierungstyps identifizieren. Nachdem Sie einen Netzwerk-Authentifizierungstyp eingegeben haben, können Sie auch die Parameter für die Datenverschlüsselung angeben. Es werden nur Netze freigegeben, die alle Parameter erfüllen.

Geben Sie im Fenster *WiFi-Netz hinzufügen* die Netzwerkdaten wie folgt ein:

**So fügen Sie einen WiFi-Link manuell hinzu:**

1 Markieren Sie im Fenster *Wifi-Netz hinzufügen* die Option **Netzwerkname**, **MAC-Adresse** oder **Authentifizierung**.

2 Wenn Sie **Netzwerkname** markiert haben, geben Sie den Namen ein und fahren Sie fort.

3 Wenn Sie **MAC-Adresse** markiert haben, geben Sie die Adresse ein und fahren Sie fort.

4 Wenn Sie **Authentifizierung** markiert haben, können Sie den Authentifizierungstyp aus dem Menü auswählen. Eventuell möchten Sie auch die **Datenverschlüsselung** definieren.

**Hinweis:** Die Optionen im Menü **Datenverschlüsselung** hängen von dem Authentifizierungstyp ab, der unter **Authentifizierung** definiert wurde. Zum Beispiel sind bei WPA-Authentifizierung die Verschlüsselungsoptionen TKIP oder AES, wohingegen bei 802.1X-Authentifizierung nur WEP-Verschlüsselung verfügbar ist.

5 Fügen Sie bei **Anmerkungen** Anmerkungen hinzu (optional).

6 Überprüfen Sie sorgfältig, ob Sie in allen Feldern die richtigen Daten eingegeben haben, und klicken Sie auf **OK**.

### 3.4.8 Löschen einer Gruppe

Sie können bei Bedarf eine Gerätegruppe oder eine WiFi-Gruppe aus der weißen Liste löschen. Dadurch wird die Gruppe mit allen ihren Mitgliedern gelöscht.

**So löschen Sie eine Gruppe:**

1 Klicken Sie auf der Registerkarte Weiße Liste mit der rechten Maustaste auf zu löschende Gruppe.

2 Klicken Sie im Menü auf **Löschen**. Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **Ja**, um die Gruppe zu löschen.

ODER

1 Wählen Sie die zu löschende Gruppe aus.

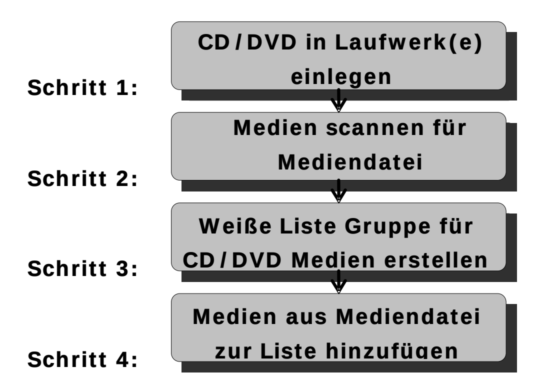
2 Klicken Sie auf die Schaltfläche **Gruppe löschen** ( ).

## 3.5 Freigeben von CD/DVD-Medien

Neben der Kontrolle von CD/DVD-Laufwerken bietet SafeGuard PortProtector die Möglichkeit, die Nutzung spezifische CD/DVD-Medien zu autorisieren. Ein besonderer Scan-Mechanismus, der so genannte Media Scanner, berechnet einen eindeutigen "Fingerprint", der die Daten auf den einzelnen Medien kennzeichnet. Jede Änderung an den Daten auf dem Medium widerruft den Fingerprint, so dass das Medium nicht mehr freigegeben ist.

Mit dieser Funktion können Administratoren die Benutzer darauf beschränken, auf ihren CD/DVD-Laufwerken nur freigegebene Medien zu nutzen. Der Administrator pflegt eine weiße Liste der freigegebenen Medien und kann darin Software-Installations-CDs mit genehmigtem Inhalt etc. aufnehmen. Der Zugriff auf diese autorisierten Medien erfolgt nur im schreibgeschützten Modus, um sicherzustellen, dass sie nach der Autorisierung unverändert bleiben.

Das folgende Diagramm zeigt, wie Medien mit Fingerprints versehen und der weißen Liste für CD/DVD hinzugefügt werden:




Das Scannen von Medien, das Erstellen von Fingerprints und das Erstellen einer Datei der gescannten Medien (Schritte 1 und 2) ist in *Appendix D – CD/DVD Media Scanner* erläutert. Die Schritte 3 und 4 werden nachstehend beschrieben.

**Hinweis:** Wenn alle CD/DVD-Laufwerke mit **Zugelassen** zugelassen sind oder ein CD/DVD-Laufwerk benutzt wird, das über die weiße Liste zugelassen ist, sind alle Medien **zugelassen**. Wenn ein Medium, das in der weißen Liste steht oder mit einem Fingerprint versehen wurde, auf einem freigebeneben CD/DVD-Gerät benutzt wird, sind darauf alle Aktionen, auch Schreiben, zugelassen. Wenn die Daten auf einem in der weißen Liste aufgeführten Medium jedoch geändert werden, wird sein Fingerprint widerrufen, und es ist nicht mehr freigegeben, wenn es auf einem mit **Eingeschränkt** eingeschränkten CD/DVD-Laufwerk benutzt wird.

Dieser Abschnitt beschreibt, wie Sie ein freigegebenes CD/DVD-Medium aus der Scanned Media-Datei hinzufügen, die Sie mit dem Media Scanner (siehe *Appendix D – CD/DVD Media Scanner*) mit Hilfe des Assistenten **Freigegebene Medien hinzufügen** (siehe *Hinzufügen eines Geräts mit Hilfe des* Assistenten) erstellt haben.

Freigegebene Medien werden der weißen Liste über die folgenden Schritten hinzugefügt:

- Hinzufügen einer Mediengruppe
- Hinzufügen einer Mediengruppe mit Hilfe des Assistent
- Hinzufügen von Log- and Alarmeinstellungen
- Speichern der Policy

## 3.5.1 Hinzufügen von Mediengruppen

Ähnlich wie bei freigegebenen Modellen und spezifischen Geräten werden auch freigegebene Medien in Gruppen angeordnet, damit Sie zusammengehörige Medien mit denselben Berechtigungen leichter verwalten können (z. B. alle Medien, die von der R&D-Gruppe benutzt werden. Bevor Sie Medien hinzufügen können, müssen Sie neue Mediengruppen hinzufügen.

**Hinweis:** Bevor Sie Mediengruppen zur Ausnahmenliste hinzufügen, müssen Sie die CD/DVD-Laufwerke auf **Einschränken** in der Registerkarte Speicherkontrolle *Allgemein* setzen.

So fügen Sie eine neue Mediengruppe hinzu:

1 Klicken Sie auf der Registerkarte Speicherkontrolle *Weiße Liste* im Bereich **Freigegebene spezifische Geräte/Medien** auf die Schaltfläche **Neu**. Ein Menü wird angezeigt.

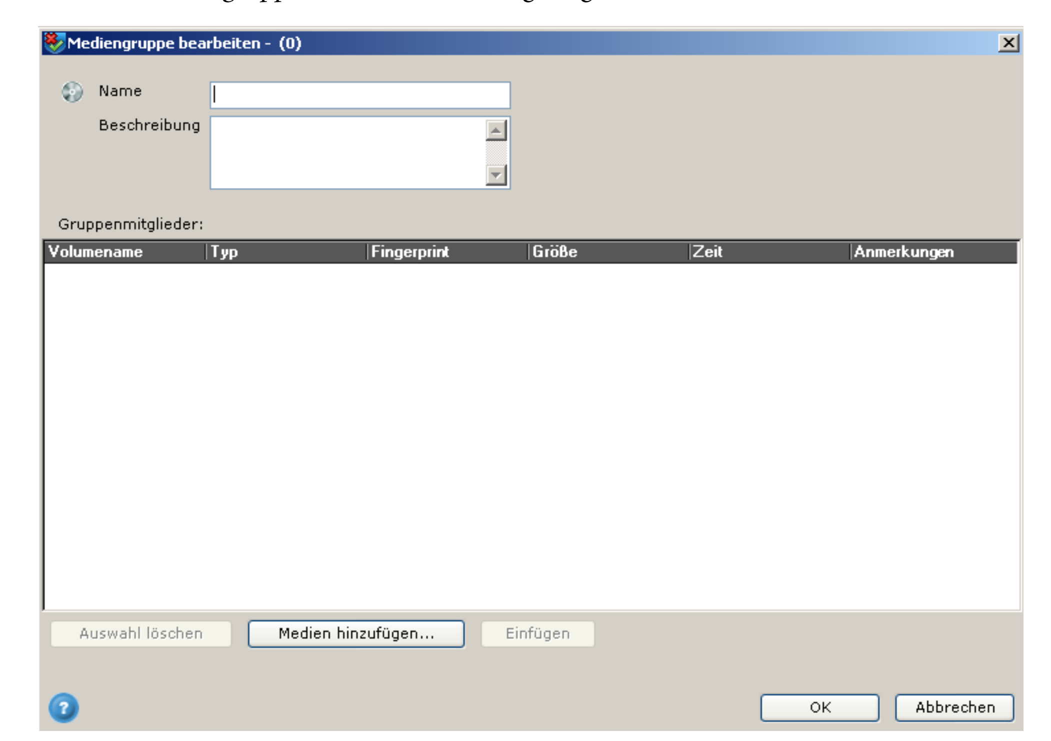
2 Wählen Sie im Menü die Option *Mediengruppe*. Das Fenster *Mediengruppe bearbeiten* wird angezeigt.

ODER

1 Klicken Sie mit der rechten Maustaste im Abschnitt **Freigegebene spezifische Geräte/Medien** auf die Registerkarte Weiße Liste. Ein Menü wird angezeigt.

2 Wählen Sie in dem Menü die Option Neue Gruppe, wählen Sie im Untermenü die Option Medien.

Das Fenster *Mediengruppe bearbeiten* wird angezeigt:




### 3.5.1.1 Hinzufügen einer Mediengruppe

Das Fenster *Mediengruppe bearbeiten* zeigt für jedes Medium in dieser Gruppe folgende Informationen an:

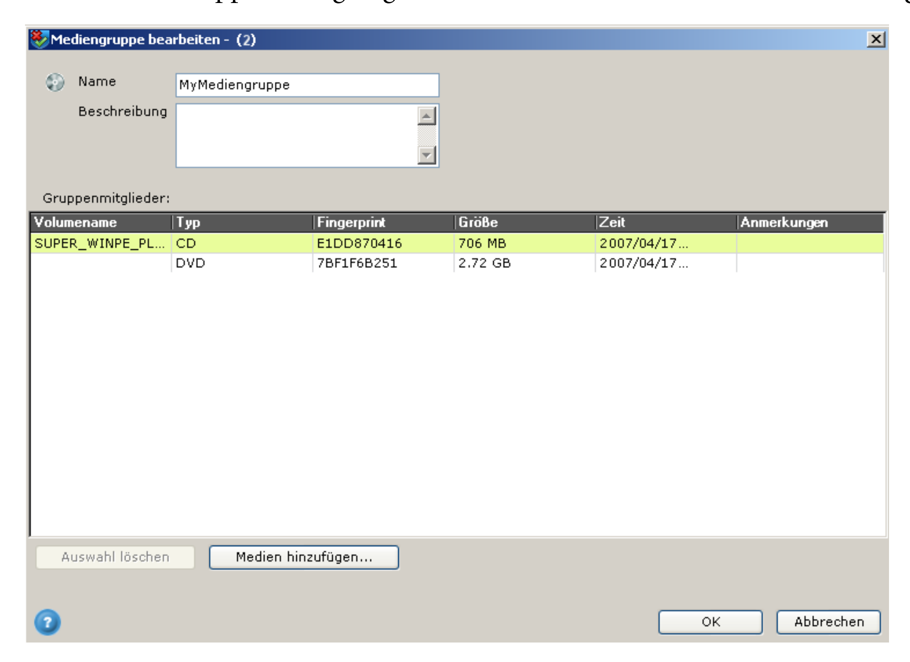
- **Volumename:** Name des gescannten Volumes, sofern eins zugeordnet wurde.
- **Typ:** CD oder DVD.
- **Fingerprint:** Der dem Medium vom Media Scanner zugewiesene Fingerprint (siehe *Appendix D – CD/DVD Media Scanner*).
- **Größe:** Größe des Inhalts auf dem Medium.
- **Zeit:** Datum und Uhrzeit, wann das Medium gescannt wurde.
- **Anmerkungen:** Eventuell von Ihnen hinzugefügte Anmerkungen.

**So fügen Sie eine CD/DVD-Mediengruppe hinzu:**

1. Mit den Schaltflächen unterhalb der Geräteliste können Sie Medien löschen oder mit Hilfe des Assistenten **Freigegebene Medien hinzufügen** (siehe *Hinzufügen eines Geräts mit Hilfe des Assistenten*) hinzufügen. Geben Sie in diesem Fenster bei **Name** (erforderlich) den gewünschten Gruppennamen und bei **Beschreibung** (optional) eine Beschreibung ein.

2. Klicken Sie auf **Medien hinzufügen**, um das Medium der Gruppe hinzuzufügen, wie in *Hinzufügen eines Geräts mit Hilfe des Assistenten* beschrieben. Alternative klicken Sie mit der rechten Maustaste auf den leeren Bereich unter **Gruppenmitglieder** und wählen **Medien hinzufügen**.

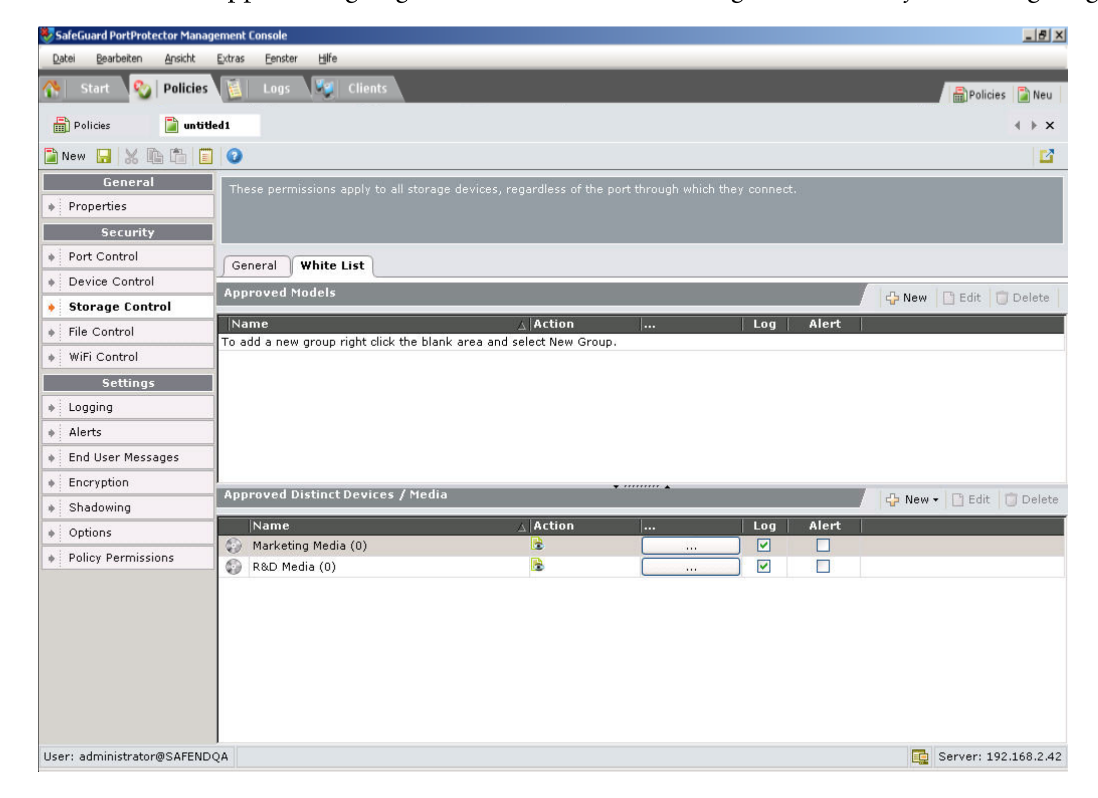
Sie können auch zu einem späteren Zeitpunkt Medien zu dieser Gruppe hinzufügen. Sobald Sie Medien zur Gruppe hinzugefügt haben, erscheinen diese im Fenster wie folgt:




3 Wenn Sie fertig sind, klicken Sie auf **OK**.

Sie können auch mit **Ausschneiden** und **Einfügen** eine Gruppe aus der Zwischenablage einfügen. Benutzen Sie hierfür die Schaltflächen **Ausschneiden** und **Einfügen** aus der Symbolleiste oder die Optionen im Menü *Bearbeiten*.

Sobald eine Gruppe hinzugefügt wurde, wird sie auf der Registerkarte *Weiße Liste* angezeigt:




In der obigen Abbildung sind zwei Mediengruppen zu sehen: *Marketing Media und R&D Media*. Die Gruppen sind automatisch auf Schreibgeschützt gesetzt, weil der Inhalt freigegebene Medien nicht verändert werden darf).

## 3.5.2 Bearbeiten einer Mediengruppe

Nachdem eine Gruppe angelegt wurde, kann sie modifiziert werden.

**So bearbeiten Sie eine Gerätegruppe:**

Doppelklicken Sie auf der Registerkarte *Weiße Liste* auf die gewünschte Gruppe.

ODER

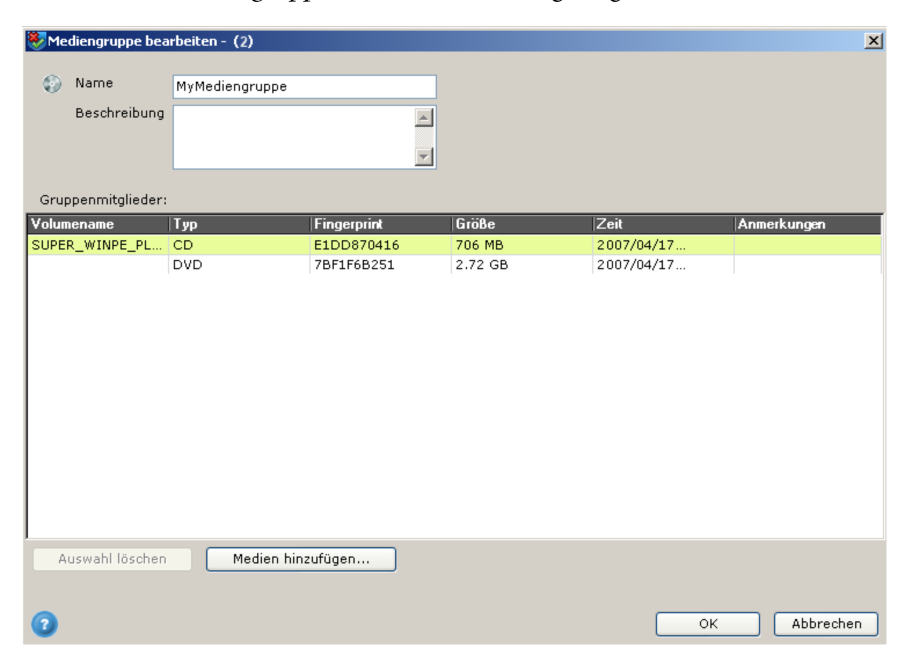
Klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe und klicken Sie dann im Menü auf **Bearbeiten**.

ODER

1 Wählen Sie die zu bearbeitende Gruppe aus.

2 Klicken Sie auf die Schaltfläche **Gruppe bearbeiten**.

Das Fenster *Mediengruppe bearbeiten* wird angezeigt:




### 3.5.2.1 Bearbeiten einer Gruppe

Falls Sie dieser Gruppe bereits Medien hinzugefügt haben, werden in dem Fenster auch die zur Gruppe gehörigen Medien angezeigt. Folgende Angaben werden für jedes Medium angezeigt:

- **Volumename:** Name des gescannten Volumes, sofern eins zugeordnet wurde.
- **Typ** CD oder DVD.
- **Fingerprint:** Der dem Medium vom Media Scanner zugewiesene Fingerprint (siehe *Appendix D – CD/DVD Media Scanner*).
- **Größe:** Größe des Inhalts auf dem Medium.
- **Zeit:** Datum und Uhrzeit, wann das Medium gescannt wurde.
- **Anmerkungen:** Eventuell von Ihnen hinzugefügte Anmerkungen.

Mit Hilfe der Schaltflächen unterhalb der Liste können Sie Medien hinzufügen oder löschen (siehe *Hinzufügen eines Geräts mit Hilfe des Assistenten*).

Die folgenden Bearbeitungsoptionen sind verfügbar:

- Hinzufügen von Medien
- Ändern von Mediendaten
- Löschen von Medien
- Kopieren von Medien in eine andere Gruppe oder Einfügen aus einer anderen Gruppe
- Ändern von Gruppen-**Name** und **Beschreibung**

## 3.5.3 Hinzufügen von Medien

Medien können vorhandenen Gruppen oder neuen Gruppen hinzugefügt werden.

**So fügen Sie ein Medium zu einer vorhandenen Gruppe hinzu:**

Klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe und wählen Sie **Zu Gruppe hinzufügen.** Der Assistent **Freigegebene Medien hinzufügen** wird geöffnet (siehe *Hinzufügen eines Geräts mit Hilfe des Assistenten).*

Eine weitere Möglichkeit, ein Medium zu einer Gruppe hinzuzufügen, haben Sie im Fenster *Gruppe bearbeiten*:

1 Öffnen Sie das Fenster Edit Group auf einem der in *Bearbeiten einer Gerätegruppe* beschriebenen Wege.

2 Klicken Sie auf **Medien hinzufügen**, und fahren Sie mit dem nächsten Abschnitt – *Hinzufügen eines Geräts mit Hilfe des Assistenten* – fort.
Wenn Sie Mediendaten aus einem Log (siehe Kopieren von USB-Geräten und CD/DVD-Mediadaten im Kapitel *Anzeigen von Logs*) kopiert haben, können Sie auch mit der rechten Maustaste auf den leeren Bereich von im Fenster *Gruppe bearbeiten* klicken und **Einfügen** wählen, um die Mediendaten in eine Gruppe zu kopieren (vergewissern Sie sich, dass Sie das Medium in eine Mediengruppe und nicht in eine Gruppe Spezifische Geräte kopieren).

Dieselben Schritte können Sie auch beim Öffnen einer neuen Gruppe verwenden, um Medien hinzuzufügen.

**Hinweis:** Falls ein Medium zu mehreren Gruppen gehört, und diese Gruppen dieselben Berechtigungen haben, wird SafeGuard PortProtector die Gruppen willkürlich auswählen. Wenn die Gruppen nicht dieselben Log- und Alarmeinstellungen haben, ist nicht vorhersehbar, welche Einstellungen angewendet werden.

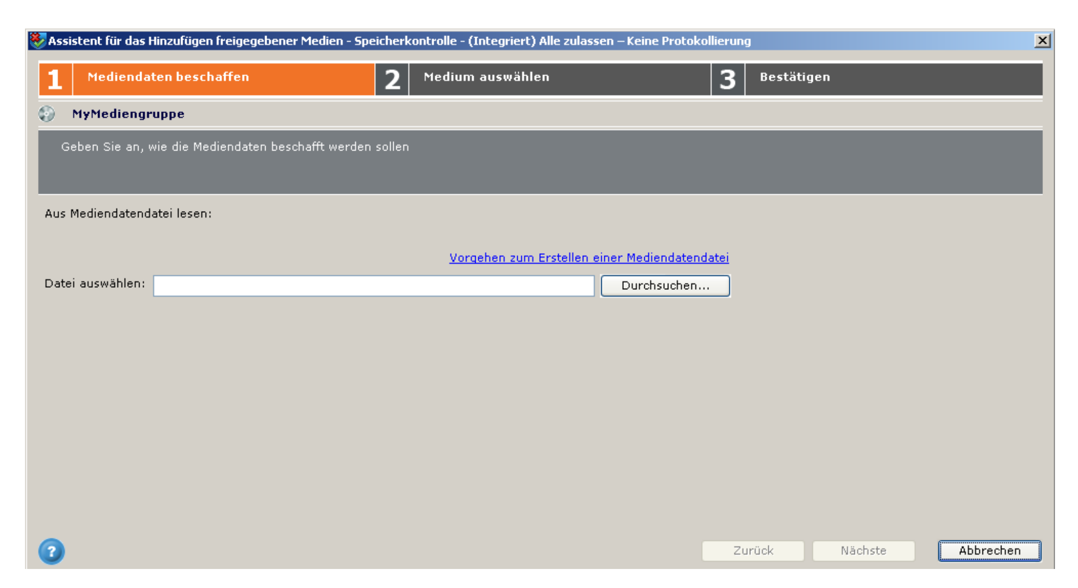
### 3.5.3.1 Hinzufügen eines Mediums mit Hilfe des Assistenten

Sobald Sie eine Mediengruppe definiert haben, steht ein einfacher Assistent **Freigegebene Medien hinzufügen** zur Verfügung. Dieser leitet Sie durch die Schritte beim Hinzufügen freigegebener Medien aus einer Liste der zuvor vom Media Scanner gescannten Medien (siehe *Appendix D – CD/DVD Media Scanner*). Der Assistent wird geöffnet, sobald Sie auf **Medien hinzufügen** im Fenster *Gruppe bearbeiten* klicken oder **Zu Gruppe hinzufügen** im Kontextmenü auswählen (siehe auch *Hinzufügen von Medien*).

Der Assistent beinhaltet drei Schritte:

- Schritt 1: Mediendaten beschaffen
- Schritt 2: Medium auswählen
- Schritt 3: Bestätigen

### 3.5.3.2 Schritt 1: Mediendaten beschaffen



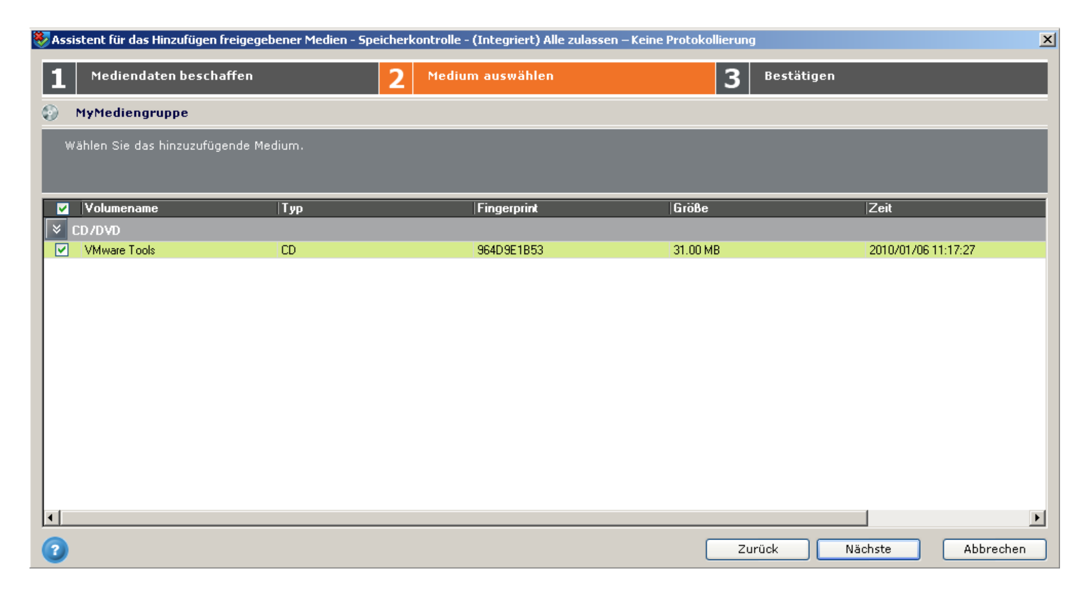

#### 3.5.3.2.1 Beschaffen von Mediendaten

In diesem Schritt können Sie die Datei angeben, aus der die Informationen über die Medien entnommen werden, die der Gruppe hinzugefügt werden sollen. Das heißt, Sie können den Speicherort der Media Scanner.XML-Datei angeben, in der die benötigten Mediendaten enthalten sind. Nachdem Sie die gewünschte Datei über **Durchsuchen** ausgewählt haben, klicken Sie auf **Nächste**, um mit Schritt 2 fortzufahren.

##### 3.5.3.2.1.1 Erstellen eine Mediendatendatei

Mit dem Media Scanner erstellen Sie eine Datei, in der eine Liste der autorisierten Medien und deren Informationen enthalten sind (die Scanned Media-Datei). Der Media Scanner scannt die gewünschten Medien und versieht sie mit Fingerprints. Die Scanergebnisse werden in einer XML-Datei gespeichert. Weitere Informationen zum Media Scanner finden Sie in *Appendix D – CD/DVD Media Scanner*.

### 3.5.3.3 Schritt 2: Medium auswählen




#### 3.5.3.3.1 Auswählen von Medien

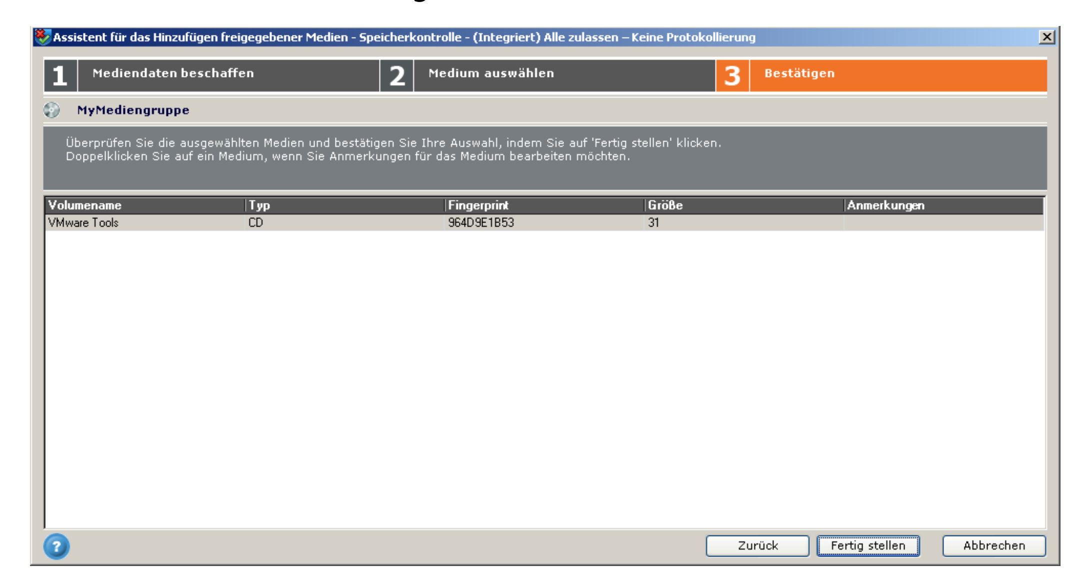
Schritt 2 zeigt eine Tabelle der mit Media Scanner gescannten und mit Fingerprints versehenen Meiden an. Zudem können Sie hier die Medien auswählen, die der Mediengruppe hinzugefügt werden sollen.

Neben jedem Medium befindet sich ein Kontrollkästchen. Markieren Sie das Kontrollkästchen, wenn Sie das Medium freigeben möchten. Medien, die bereits zur aktuellen Gruppe gehören, sind grau markiert und das Kontrollkästchen daneben ist bereits markiert.

**Hinweis:** Falls ein Medium zu mehreren Gruppen gehört, und diese Gruppen dieselben Berechtigungen haben, wird SafeGuard PortProtector die Gruppen willkürlich auswählen. Wenn die Gruppen nicht dieselben Log- und Alarmeinstellungen haben, ist es nicht vorhersehbar, welche Einstellungen angewendet werden.

Sobald Sie die der Gruppe hinzuzufügenden Medien ausgewählt haben, klicken Sie auf **Nächste**, um mit Schritt 3 fortzufahren.

### 3.5.3.4 Schritt 3: Bestätigen




#### 3.5.3.4.1 Bestätigen der Auswahl

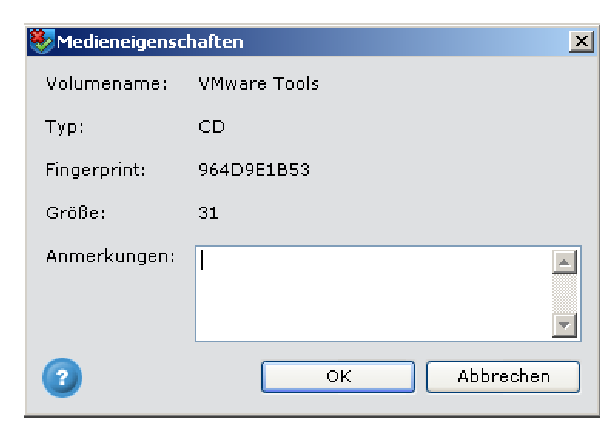
Hier überprüfen Sie die Gruppe mit ihren neu hinzugefügten Medien und bestätigen Ihre Auswahl. Vor dem Bestätigen können Sie Anmerkungen zu einem Medium hinzufügen, wie in *Hinzufügen von Anmerkungen zu den Medieneigenschaften* weiter unten erläutert.

**So bestätigen Sie Ihre Auswahl:**

1 Um Anmerkungen zu den Eigenschaften eines Mediums hinzuzufügen, doppelklicken Sie auf das Medium.

ODER

Klicken Sie mit der rechten Maustaste auf das Medium, und klicken Sie dann auf **Bearbeiten**. Das Fenster *Medieneigenschaften* wird angezeigt:




Weitere Anleitungen hierzu finden Sie in *Hinzufügen von Anmerkungen zu den Medieneigenschaften* weiter unten.

2 Zur Bestätigung der Medienauswahl klicken Sie auf **Fertig stellen**. Oder klicken Sie auf **Zurück**, um zum vorherigen Stadium zurückzukehren.

###### 3.5.3.4.1.1 Hinzufügen von Anmerkungen zu den Medieneigenschaften

Geben Sie im Fenster *Medieneigenschaften* die gewünschten Anmerkungen ein, und klicken Sie auf **OK**.

## 3.5.4 Weitere Einstellungen für Mediengruppen

Nachdem Sie die gewünschten Medien zu einer Gruppe hinzugefügt haben, müssen Sie noch einige Einstellungen definieren:

### 3.5.4.1 Log- and Alarmeinstellungen

**So definieren Sie Log- and Alarmeinstellungen:**

Markieren Sie bei Bedarf für jede Gruppe die Kontrollkästchen *Log* und *Alarm*.

Hinweis: Aus diesem Grund ist **Aktion** für die Gruppe Freigegebene Medien immer auf Schreibgeschützt gesetzt.

### 3.5.4.2 Berechtigungen für Mediengruppen

Die Berechtigungen für Mediengruppen können nicht konfiguriert werden, weil die Dateikontrolle nicht auf freigegebene Medien angewandt wird. Das bedeutet, dass nach der Freigabe jede Art von Datei von diesen Medien gelesen werden kann.

## 3.6 Verwalten von Policies

Das unten gezeigte Fenster *Policies* ist der zentrale Punkt, an dem Sie eine Liste Ihrer Policies anzeigen und verschiedene Aktionen durchführen können, wie etwa das Bearbeiten, Löschen, Exportieren von Policies etc.

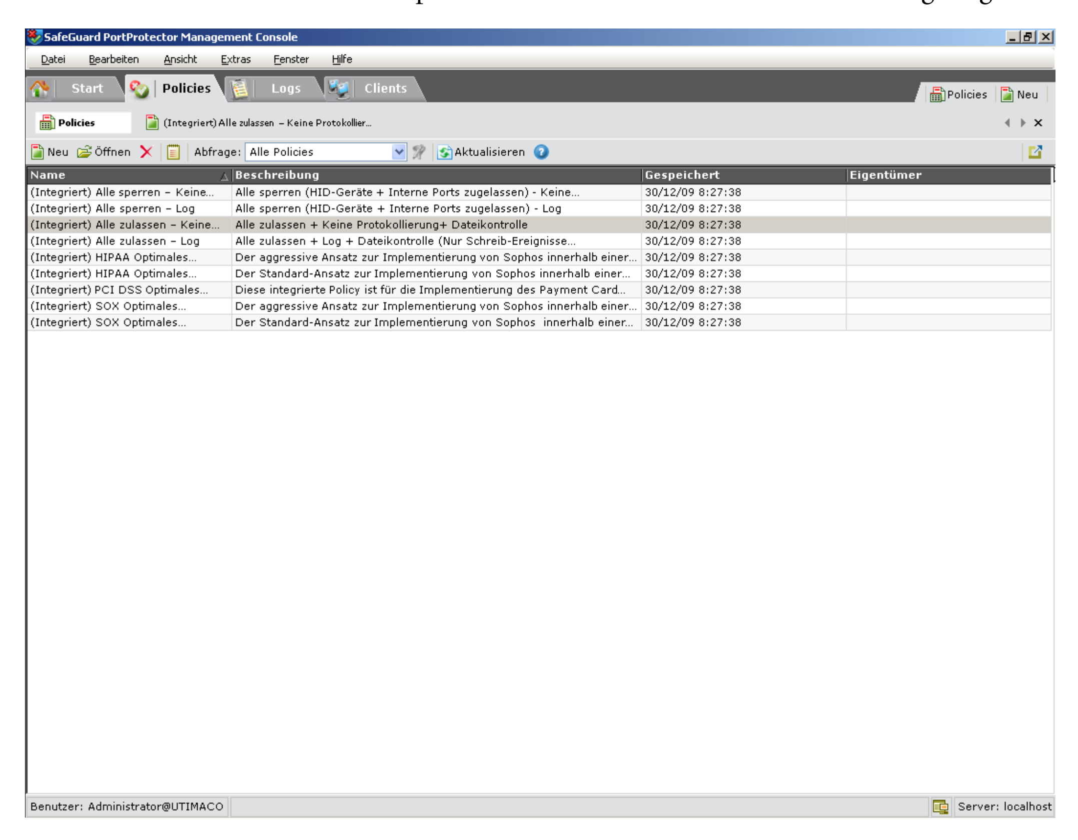
Dieses Fenster wird automatisch angezeigt, wenn Sie anfangs die Policies-Welt öffnen, indem Sie auf die Registerkarte *Policies* klicken. Nachdem Sie zu anderen Fenstern in der Policies-Welt gewechselt haben, können Sie zum Fenster *Policies* auf verschiedenen Wegen zurückkehren:

**So öffnen Sie das Fenster Policy-Management (*Policies*):**

Klicken Sie in der Fensterleiste oder in der oberen rechten Ecke des Fensters auf das Symbol **Policies** (Policies).

ODER

Wählen Sie im Menü Datei die Option **Policies.** Das Fenster Policies wird angezeigt.




SafeGuard PortProtector Management Console verfügt über mehrere integrierten Policies. Eine Beschreibung hierzu finden Sie in *Schritt 3: Policy erstellen*.

Im Fenster *Policies* können Sie folgende Aktionen ausführen:

- Öffnen einer Policy, erläutert in *Öffnen einer Policy*.
- Ändern einer Policy, erläutert in *Ändern einer Policy*.
- Erstellen einer neuen Policy, erläutert in *Erstellen einer neuen Policy*.
- Löschen einer Policy, erläutert in *Löschen von Policies*.
- Anzeigen und Drucken einer Policy-Übersicht (siehe auch *Anzeigen und Drucken einer Policy-Übersicht*).

- Exportieren oder Importieren einer Policy in/aus einer Datei (siehe auch *Exportieren und Importieren einer Policy*).
- Abfrage der mit einem Organisationsobjekt verknüpften Policies, erläutert in *Abfragen zugehöriger Policies*.

### 3.6.1 Öffnen einer Policy

Sie können eine vorhandene Policy über das Fenster *Policies* öffnen.

**So öffnen Sie eine Policy:**

Doppelklicken Sie im Fenster *Policies* auf die zu öffnende Policy

ODER

Klicken Sie mit der rechten Maustaste auf die Policy und wählen Sie **Öffnen**.

ODER

Klicken Sie in der Symbolleiste auf die Schaltfläche **Öffnen** (Öffnen).Das Fenster Policy wird mit den Definitionen der Policy angezeigt.

### 3.6.2 Ändern einer Policy

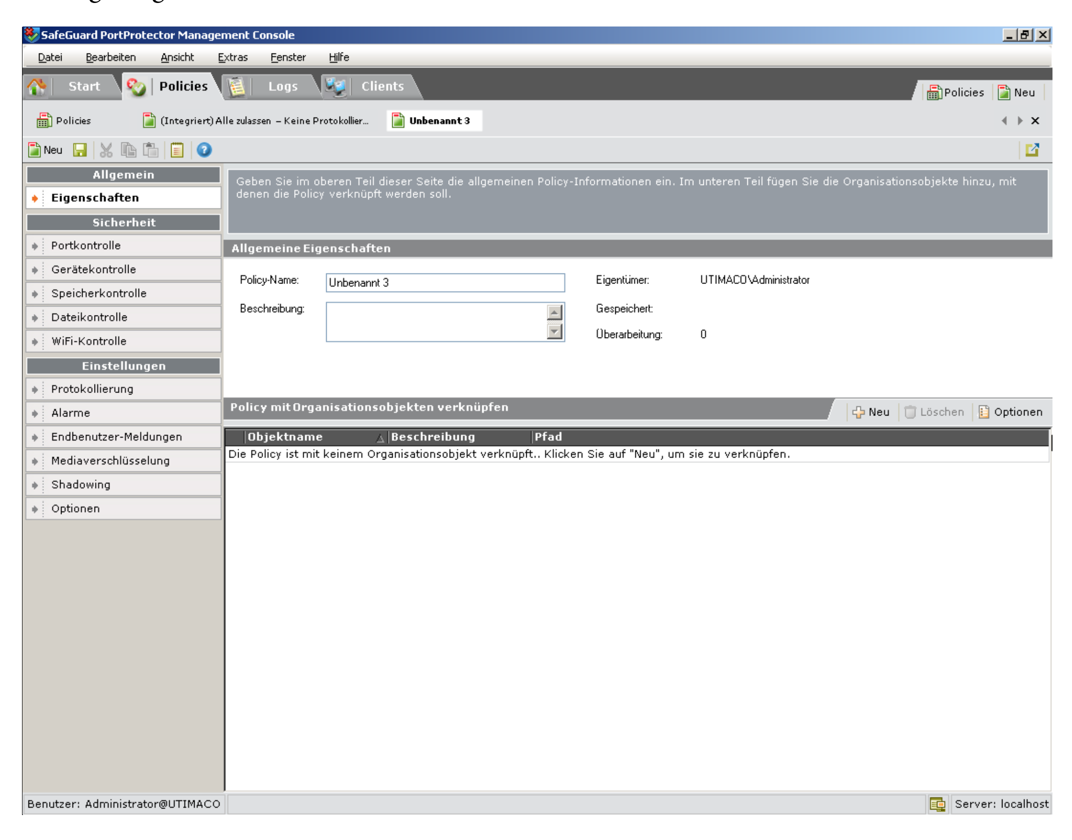
Nachdem Sie eine Policy geöffnet haben, können Sie ihre Definitionen ändern und speichern, oder diese als eine neue Policy unter einem anderen Namen speichern.

## 3.6.3 Erstellen einer neuen Policy

Die verschiedenen Wege für das Öffnen einer neuen Policy sind in *Schritt 3: Policy erstellen* erläutert. eine weitere Möglichkeit zum Öffnen einer neuen Policy ist über das Fenster *Policy-Management*.

**So erstellen Sie eine neue Policy von aus den Standardeinstellungen:**

Klicken Sie mit der rechten Maustaste auf das Fenster *Policy-Management*, und wählen Sie **Neu**. Es wird eine unbenannte Policy mit Standardeinstellungen geöffnet. Das folgende Fenster ist das anfänglich geöffnete Fenster:




Dieses Fenster ist in zwei Abschnitte unterteilt:

- **Allgemeine Eigenschaften:** der obere Abschnitt. Hier geben Sie den Namen der neuen Policy und ihre Beschreibung ein (unten erläutert). Dieser Abschnitt zeigt auch den Eigentümer (ein Administrator) der Policy, den Zeitpunkt der letzten Speicherung und der letzten Überarbeitung.
- **Policy mit Organisationsobjekten verknüpfen:** der untere Abschnitt. Hier verknüpfen Sie die Policy mit Organisationsobjekten. Eine Erklärung finden Sie in *Verteilen von SafeGuard PortProtector Policies direkt vom Management Server aus* in *Kapitel 4, Verteilen von Policies*.

**So geben Sie den Namen und die Beschreibung der Policy ein:**

Geben Sie im Abschnitt Allgemeine Eigenschaften den Namen und die Beschreibung der Policy ein.

Anschließend können Sie die Einstellungen für die Policy definieren und sie speichern.

### 3.6.4 Löschen von Policies

Sie können nicht mehr benötigte Policies löschen. Durch das Löschen von Policies werden diese aus dem Active Directory und aus der Management Console entfernt. Mit Hilfe der **Strg**-Taste können Sie eine Mehrfachauswahl der zu löschenden Policies treffen.

**Hinweis:** Wenn Policies in der Management Console gelöscht werden, sind sie noch nicht auf dem SafeGuard PortProtector Client gelöscht, auf dem sie aktiv sind. Somit ist die Sicherheit Ihrer Organisation nicht gefährdet.

**Hinweis:** Wir raten dringend davon ab, Policies zu löschen, die für Computern und/oder Benutzer in Ihrer Organisation gelten. Denken Sie vor dem Löschen daran, dass Sie nach dem Löschen keine Aufzeichnung der Policy-Definitionen mehr haben. Außerdem müssen Sie dann, wenn Sie irgendwann einmal die Policy auf den durch diese Policy geschützten Clients aktualisieren müssen, eine neue Policy erstellen.

So löschen Sie Policies:

Klicken Sie im Fenster *Policy-Management* mit der rechten Maustaste auf die zu löschende Policy und wählen Sie **Löschen**.

ODER

Klicken Sie in der Symbolleiste auf die Schaltfläche **Löschen** (✕). Nach erfolgter Bestätigung wird die Policy gelöscht

### 3.6.5 Anzeigen und Drucken einer Policy-Übersicht

Sie können nicht nur durch die verschiedenen Fenster blättern, in denen die Policy-Einstellungen in definiert sind, sondern auch die Einstellungen der Policy in einem einzelnen Fenster anzeigen und drucken.

**So zeigen Sie die Policy-Übersicht an:**

Klicken Sie im Fenster *Policy-Management* mit der rechten Maustaste auf die anzuzeigende Policy, und wählen Sie **Übersicht anzeigen**.

ODER

Klicken Sie in der Symbolleiste auf die Schaltfläche **Übersicht anzeigen** ( ).

ODER

Wählen Sie die Policy aus, und klicken Sie auf **Policy-Übersicht** im Menü *Datei*.

Das Fenster *Policy-Übersicht* wird angezeigt:




### 3.6.5.1 Policy-Übersicht

In diesem Fenster können Sie die Policy-Übersicht anzeigen und drucken.

**So drucken Sie die Policy-Übersicht:**

Klicken Sie im Fenster *Übersicht* mit der rechten Maustaste, und wählen Sie im Menü die Option **Drucken**.

## 3.6.6 Exportieren und Importieren einer Policy

Eventuell möchten Sie Policies aus der Policy-Datenbank in eine Datei auf Ihrem Computer exportieren, damit Sie sie zu einem späteren Zeitpunkt nutzen können (wenn Sie z. B. die in Ihrer Testversion der Management Console definierten Einstellungen speichern möchten, um sie später im lizenzierten Produkt zu verwenden). Nachdem Sie die Policy exportiert haben, können Sie diese zu einem späteren Zeitpunkt in die Datenbank importieren.

**So exportieren Sie eine Policy:**

1 Klicken Sie im Fenster *Policy-Management* mit der rechten Maustaste auf die zu exportierende Policy und wählen Sie **Exportieren**.

ODER

Klicken Sie im Menü *Datei* auf die Option **Exportieren**.

Das Fenster *Policy exportieren* wird angezeigt.

2 Wählen Sie den gewünschten Dateinamen und den Speicherort aus, und klicken Sie auf **Speichern.**

**So importieren Sie eine Policy:**

3 Klicken Sie mit der rechten Maustaste auf das Fenster *Policy-Management* und wählen Sie **Importieren**.

ODER

Klicken Sie im Menü *File* auf die Option **Importieren**.

Das Fenster *Policy importieren* wird angezeigt.

4 Wählen Sie die gewünschte Datei und klicken Sie auf Open. Die importierte Policy wird geöffnet.

5 Zum Speichern der Policy verwenden Sie die Option **Speichern** oder **Speichern unter** im Menü *Datei*.

## 3.6.7 Abfragen zugehöriger Policies

Wenn Sie Policies über die Option Policy-Server mit Organisationsobjekten verknüpft haben (siehe *Verteilen von SafeGuard PortProtector Policies direkt vom Management Server aus* in *Kapitel 4, Verteilen von Policies*), können Sie SafeGuard PortProtector Clients daraufhin abfragen, welche Policies mit einem Benutzer/Computer verknüpft sind. Anhand dieser Informationen können Sie herausfinden, welche Berechtigungen tatsächlich für den Benutzer/Computer in Kraft sind, und ob er mit einer oder mehreren Policies verknüpft ist.

**So zeigen Sie mit den angegebenen Objekten verknüpfte Policies an:**

1 Wählen Sie im Fenster *Policies* im unten dargestellten Menü *Abfrage*, das in der Symbolleiste erscheint, die Option **Nach verknüpftem Objekt** (die andere, standardmäßige, Option ist Alle Policies).




2 Das Fenster *Objekt auswählen* wird angezeigt: (Eine detaillierte Beschreibung dieses Fensters finden Sie unter *Verknüpfen einer Policy mit Organisationsobjekten* in *Kapitel 4, Verteilen von Policies*).

**Hinweis:** Das Menü *Abfrage* wird im Fenster *Policies* nur angezeigt, wenn die Option Policy Server aktiviert ist. Weitere Informationen zu dieser Option finden Sie in *Verteilen von SafeGuard PortProtector Policies direkt vom Management Server aus* im Kapitel *Verteilen von Policies*.

3 Filtern Sie das Fenster *Objekte* nach Bedarf (wie in *Auswählen und Verknüpfen von Objekten nach Namen* und *Filtern von Objekten unter Verwendung der Organisationsstruktur* im Kapitel *Verteilen von Policies*, erläutert).

**Hinweis:** Im Gegensatz zum Filtern von Objekten bei der Policy-Zuweisung enthält das Menü *Objekttyp* bei der Abfrage verknüpfter Policies nur die Optionen Computer und Benutzer.

4 Klicken Sie auf **LOS** . Das Fenster *Objekte* zeigt auf der rechten Seite dann eine Liste aller Objekte, die den Filterkriterien entsprechen.

5 Wählen Sie aus der Liste der Objekte das Objekt aus, für das Sie die verknüpften Policies anzeigen möchten. Markieren Sie dazu das entsprechende Kontrollkästchen.

**Hinweis:** Da der Zweck der Abfrage darin liegt, die mit dem einen, angegebenen Objekt verknüpften Policies anzuzeigen, kann jeweils nur ein Objekt ausgewählt werden.

6 Klicken Sie zur Anzeige der Policies auf **OK**. Im Fenster *Policies* werden dann nur die mit dem ausgewählten Objekt verknüpften Policies angezeigt.

**So zeigen Sie wieder alle Policies an:**

Wählen Sie im Fenster *Policies* im Menü *Abfrage* die Option Alle Policies. Im Fenster *Policies* werden jetzt alle Policies angezeigt.

## 3.7 Optionen für aktives Fenster

Das aktive Policy-Fenster kann dupliziert, gelöst und geschlossen werden. Diese Optionen sind in *Optionen für aktives* Fenster im Kapitel *Erste Schritte*, beschrieben.

# 4 Verteilen von Policies

## Über dieses Kapitel

Dieses Kapitel beschreibt die Verteilung von SafeGuard PortProtector-Policies zum Schutz der Endpunkte in Ihrer Organisation.

- ***Übersicht*** beschreibt die Optionen der Verteilung von SafeGuard PortProtector-Policies – direkt vom Management Server aus über SSL (Policy Server), über Active Directory oder als Registry-Dateien (für die allgemeine Nutzung durch Tools von Drittanbietern).
- ***Verteilen von SafeGuard PortProtector Policies direkt vom Management Server aus*** beschreibt, wie Policies über die Management Console mit Organisationsobjekten verknüpft werden, so dass sie direkt von den Servern an die SafeGuard PortProtector Clients verteilt werden können.
- ***Verteilen von SafeGuard PortProtector-Policies unter Verwendung von Active Directory*** beschreibt, wie SafeGuard PortProtector-Policies (GPOs) zu den Computern und Benutzern in Ihrer Organisation zugewiesen werden, und wie Sie die erforderlichen SafeGuard PortProtector-Policies finden.
- ***Verteilung von SafeGuard PortProtector Policies unter Verwendung von Registry-Dateien*** beschreibt, wie SafeGuard PortProtector-Policies als Registry-Dateien in einem freigegebenen Ordner gespeichert werden, damit Sie durch Tools von Drittanbietern an die SafeGuard PortProtector Clients verteilt werden können. Mit dieser Option können Sie Policies in Novell eDirectory importieren und sie mit den Funktionen von eDirectory verteilen.
- ***Zusammenführen von Policies*** beschreibt, wie SafeGuard PortProtector Policies bei Bedarf zusammenführt.

## 4.1 Übersicht

SafeGuard PortProtector bietet drei Verfahren für das Deployment von Policies:

- **Direkt vom Management Server aus** (diese Funktion wird auch als Policy Server bezeichnet): Mit dieser Option können Sie Policies direkt in der Management Console mit Organisationsobjekten verknüpfen. Nach der Zuweisung werden die Policies vom Management Server direkt über SSL an die SafeGuard PortProtector Clients verteilt.
- **Unter Verwendung von Active Directory:** Bei dieser Option wird der standardmäßige GPO-Verteilungsmechanismus von Active Directory zur Verteilung von Policies genutzt, wie weiter unten beschrieben. Dies ist die Standardoption. In diesem Fall erzeugt (veröffentlicht) SafeGuard PortProtector automatisch jede Policy, die Sie in der SafeGuard PortProtector Management Console definieren, als ein GPO in Active Directory. Diese Policies werden dann automatisch von Active Directory an die Computer und Benutzer verteilt, die zu der Organisationseinheit (OU) gehören, der Sie sie zuweisen möchten.
- **Unter Verwendung von Registry-Dateien in einem freigegebenen Ordner:** Diese Option veröffentlicht, oder speichert, Policies als Registry-Dateien in einem freigegebenen Ordner und ermöglicht es Ihnen, die Policy auf den Clients manuell zu aktualisieren oder SafeGuard PortProtector-Policies mit Hilfe von Fremdtools an die SafeGuard PortProtector Clients zu verteilen. Weitere Informationen finden Sie in Veröffentlichungsmethode im Kapitel *Administration*.

## 4.2 Verteilen von SafeGuard PortProtector Policies direkt vom Management Server aus

Eine der wesentlichsten Stärken von SafeGuard PortProtector ist seine weitreichende Integration in vorhandene IT-Infrastrukturen. Nach der Installation erkennt das Produkt automatisch das Netz, stellt die Verbindung zu Active Directory (AD) her und führt die Synchronisierung (schreibgeschützt) mit der vorhandenen Organisationsstruktur inklusive Organisationseinheiten, Gruppen, Benutzern und Computern durch. Mit diesem Vorgehen kann der Administrator seine AD-Objekte in nativer Form bei der Ausführung von Aufgaben in der SafeGuard PortProtector Management Console nutzen. Darüber hinaus kann das System diese skalierbare Architektur mit hoher Verfügbarkeit ausnutzen und Policies über den GPO-Mechanismus von AD an die Endpunkte verteilen. Jedoch ist für die Zuweisung der Policy-Objekte zu Benutzern und Computern einiges Wissen seitens der Benutzer erforderlich.

Ein weiteres Verfahren für die Verteilung von Policies an Endpunkte ist der Policy Server. Mit dieser Funktion werden Policies direkt vom Management Server über die vorhandene SSL-Infrastruktur an die Endpunkte verteilt. Zur Vereinfachung werden Policies in der Management Console im Rahmen der Definition der Policy mit AD- oder Novell-Objekten verknüpft. Dabei können sowohl allgemeiner gehaltene Policies (für Organisationseinheiten oder Gruppen) als auch für einen bestimmten Benutzer oder Computer geltende Policies festgelegt werden.

### 4.2.1 Architektur

Wenn der Policy Server als Schleuse für die Verteilung von Policies konfiguriert wurde, fragen die Endpunkte den Management Server nach den ihnen zugewiesenen Policies ab. Diese Abfrage erfolgt jedes Mal, wenn ein Computer startet, wenn sich ein Benutzer anmeldet, sowie in vordefinierten Zeitintervallen. Diese Kommunikation ähnelt sehr dem Verfahren bei dem Logs von Endpunkten zu Servern gesendet werden. Dieses Verfahren basiert auf Web-Server und setzt SSL zur Authentifizierung und Verschlüsselung ein. Außer den bereit für die Log-Erfassung genutzten Ports brauchen keine neuen Ports geöffnet zu werden.

Um eine hohe Performance, Skalierbarkeit und minimal Netzbelastung, sicherzustellen, wurden viele Optimierungen eingebracht, einschließlich Komprimierung der Policies, serverseitiges Caching und Snapshots.

### 4.2.2 Verknüpfen von Policies mit Organisationsobjekten

Die Benutzeroberfläche für die Definition der Policies ermöglicht die Verknüpfung einer Policy mit AD-/Novell-Objekten. Diese Oberfläche lässt die Zuweisung einer Policy zu mehreren Objekten verschiedener Typen zu. Zusätzliche Funktionen bestehen für das Suchen nach Objekten entweder nach Namen oder über die Navigation durch die Organisationsstruktur.

Policies können mit einem oder mehreren der folgenden AD-/Novell-Objekte verknüpft werden:

- Domäne
- Organisationseinheit (OU)
- Gruppe
- Benutzer
- Computer

**Hinweis:** Mit dem Policy Server können auch Computer, die nicht über AD/Novell verwaltet werden (nicht in der Domäne sind), mit Policies verknüpft werden und Policy-Aktualisierungen direkt vom Management Server erhalten.

Der Policy Server bringt die Funktion der Policy-Zusammenführung des SafeGuard PortProtector Clients ein. Dank dieser Funktion kann der Benutzer mehrere Policies mit einem Objekt verknüpfen, so dass der Client einen vereinten Satz an Berechtigungen aus all diesen Policies durchsetzt. Das Zusammenführen von Policies ist in *Zusammenführen von Policies* beschrieben.

### 4.2.3 Verknüpfen einer Policy mit Organisationsobjekten

Die Verknüpfung einer Policy mit Organisationsobjekten zur Anwendung der Policy auf diese Objekte besteht aus folgenden Schritten:

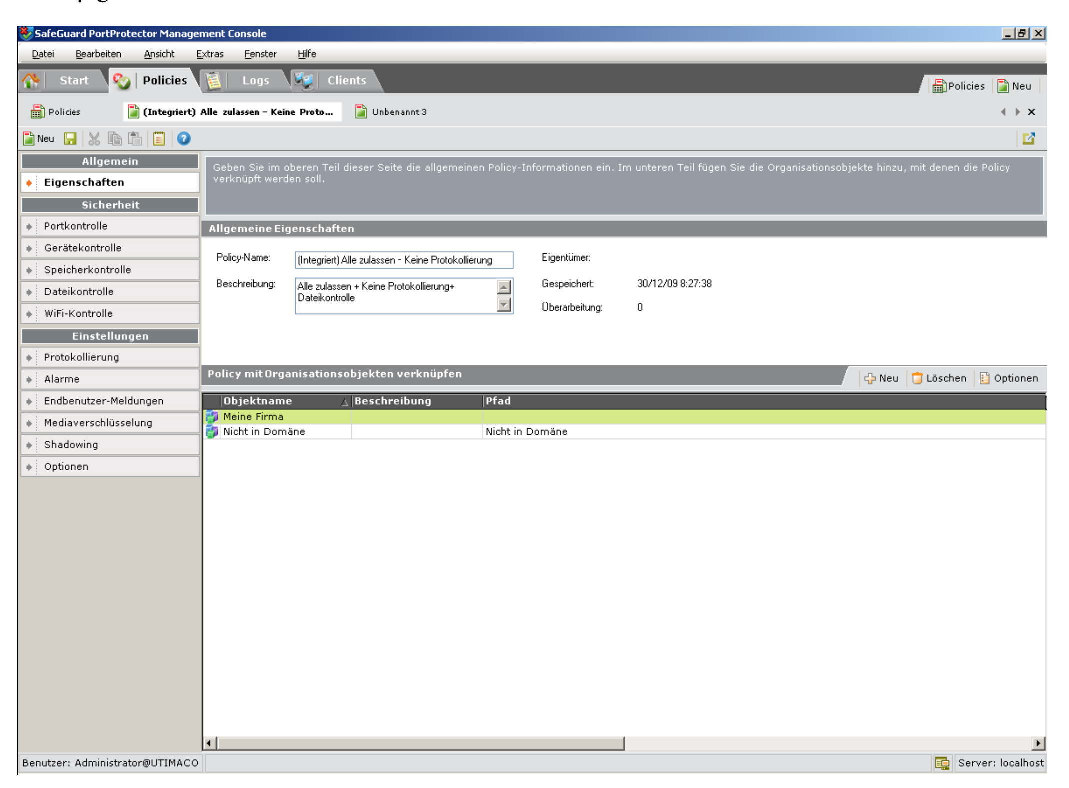
- **Öffnen des Fensters *Objekt auswählen***: beschrieben in *Öffnen* des Fensters Objekt auswählen.
- **Filtern von Objekten und Auswählen von Objekten für die Policy-Verknüpfung:** beschrieben in *Filtern und Verknüpfen von Objekten*.
- **Einschränken der Policy auf Benutzer/Computer**: beschrieben in *Einschränken der Policy auf Benutzer/Computer*.

Die Verknüpfung einer Policy mit Organisationsobjekten erfolgt im Fenster *Objekt auswählen*, auf das Sie über die Registerkarte *Properties* der Policy zugreifen. Im Fenster *Objekt auswählen* werden Organisationsobjekte angezeigt, aus denen Sie die gewünschten Objekte auswählen können. In diesem Fenster können Sie die Organisationseinheiten so filtern, dass die Liste der Objekte, aus der Sie die verknüpften Objekte auswählen, Ihren Anforderungen entspricht (wenn Sie zum Beispiel eine Policy mit Benutzern in einer bestimmten Domäne verknüpfen möchten, ist es nicht notwendig, andere Domänen oder Computer in der Domäne anzuzeigen).

Hinweis: Bevor mit der Verknüpfung begonnen wird, müssen Sie **Policies direkt vom Server an die Clients veröffentlichen** im Fenster *Administration* wählen (siehe Veröffentlichungsmethode im Kapitel *Administration*).

### 4.2.3.1 Öffnen des Fensters Objekt auswählen

Das Fenster *Objekt auswählen* wird über die unten gezeigte Registerkarte *Eigenschaften* der Policy geöffnet:




#### 4.2.3.1.1 Fenster Policy-Eigenschaften

In diesem Fenster können Sie den Namen und eine Beschreibung für die Policy eingeben. Eine neue Policy enthält die Standardwerte oder die Werte der Policy-Vorlage, sofern Sie eine solche Vorlage definiert haben (siehe *Policy-Vorlage* im Kapitel *Administration*).

Wenn Sie wählen, Policies direkt vom Management Server aus an die Clients zu veröffentlichen (siehe *Veröffentlichungsmethode* im Kapitel *Administration*), werden im Fenster *Eigenschaften* die Organisationsobjekte angezeigt, mit denen diese Policy verknüpft ist. Es zeigt den Objektnamen, ggf. die Beschreibung und den Pfad. Mit Hilfe der Schaltflächen **Neu** und **Löschen** können Sie Objekte zur Liste der verknüpften Objekte hinzufügen oder daraus löschen. Anleitungen für das Auswählen von Objekten zur Verknüpfung finden Sie unten in *Auswählen eines Objekts zur Verknüpfung*.

### 4.2.3.2 Auswählen eines Objekts zur Verknüpfung

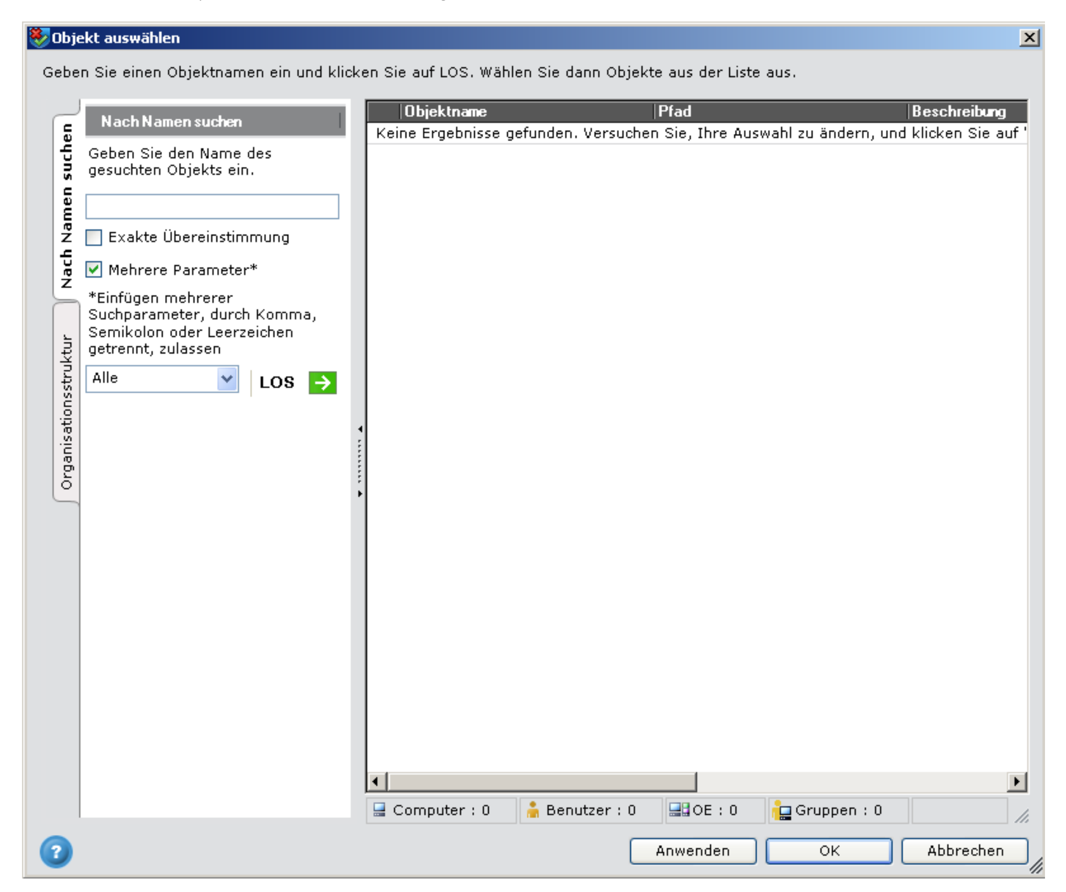
**So öffnen Sie das Fenster *Objekt auswählen*:**

Klicken Sie im unteren Abschnitt des Policy-Fensters *Eigenschaften* (Abschnitt Policy mit Organisationsobjekten verknüpfen) auf **Neu**.

ODER

Klicken Sie mit der rechten Maustaste in den unteren Abschnitt des Fensters (Policy mit Organisationseinheiten verknüpfen).

Das Fenster *Objekt auswählen* wird geöffnet:




Das Fenster *Objekt auswählen* zeigt die Registerkarten *Nach Namen suchen* und *Organisationsstruktur* auf der linken Seite. Die rechte Seite enthält die Tabelle der Objekte. Die Registerkarten helfen Ihnen bei der Auswahl der gewünschten Objekte, mit denen die Policy verknüpft werden soll. Die Registerkarten enthalten auch eine Dropdown-Liste (das Menü *Objekttyp*), über die Sie festlegen können, welche Objekttypen in der Tabelle gezeigt werden sollen. Die Objekttabelle zeigt das Ergebnis Ihre Auswahl an. Aus den angezeigten Objekten können Sie anschließend die zu verknüpfenden Objekte auswählen.

### 4.2.3.3 Filtern und Verknüpfen von Objekten

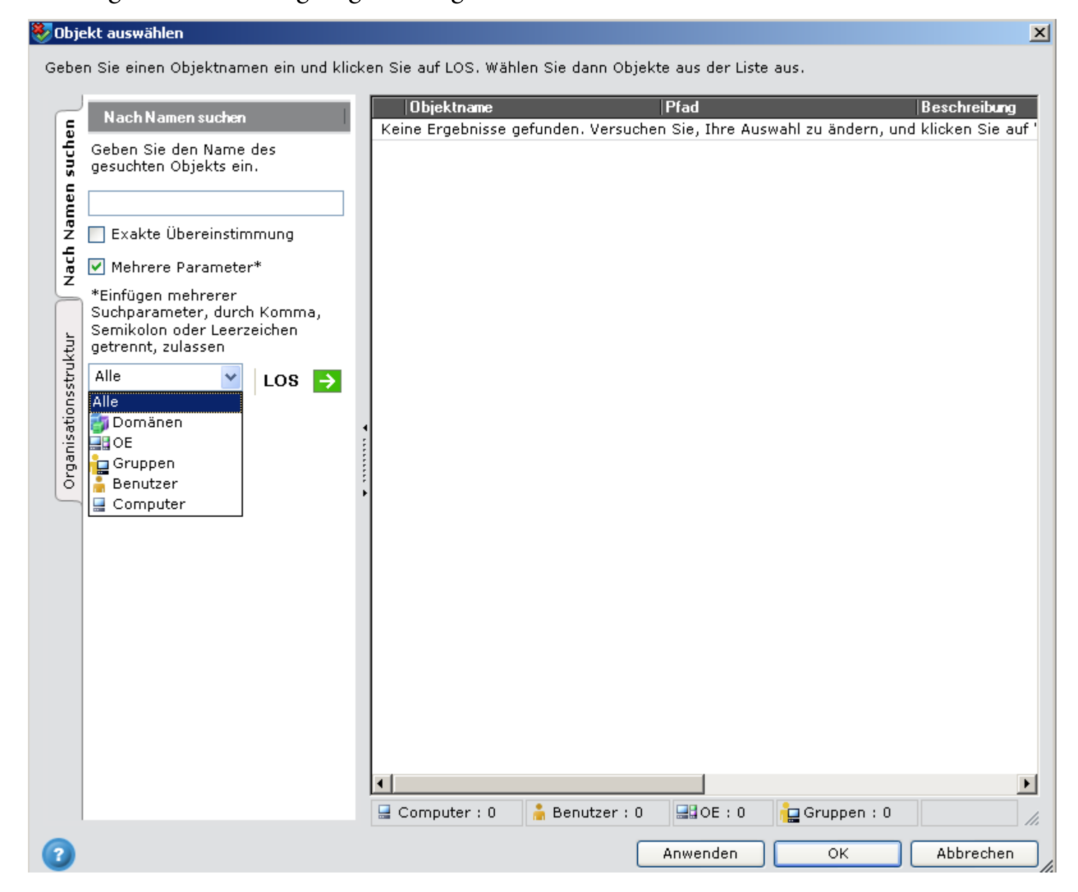
Die linke Seite des Fensters *Objekt auswählen* enthält zwei Registerkarten, in denen Sie festlegen können, welche Organisationsobjekte im Fenster angezeigt werden, und aus denen Sie die mit der Policy zu verknüpfenden Objekte auswählen. Dabei handelt es sich um die Registerkarten *Nach Namen suchen* und *Organisationsstruktur*.

**Hinweis:** Wenn die Funktion der Domänenpartitionierung aktiviert ist (siehe *Definieren von Domänenpartitionen*), werden nur die der Rolle dieses Benutzers zugewiesenen Organisationseinheiten angezeigt.

#### 4.2.3.3.1 Filtern von Objekten nach Namen

Die Registerkarte *Nach Namen suchen* ist ein Tool, mit dessen Hilfe Sie die anzuzeigenden Organisationsobjekte (Organisationseinheiten, Gruppen, Computer, Benutzer etc.) festlegen können. Durch die Suchkriterien, die Sie hier eingeben, werden die in der *Objekte*tabelle angezeigten Objekte bestimmt. Nachdem Sie diese Objekte ausgewählt und angezeigt haben, können Sie angeben, welche der angezeigten Objekte mit der Policy verknüpft werden sollen.

Die folgende Abbildung zeigt die Registerkarte *Nach Namen suchen*:




##### 4.2.3.3.1.1 Auswählen und Verknüpfen von Objekten nach Namen

**Hinweis:** Die Anleitungen in diesem Abschnitt beziehen sich auch auf das Abfragen zugehöriger Policies nach Namen. In diesem Fall werden als Ergebnis Ihrer Auswahl im Fenster *Policies* die Policies angezeigt, die mit den ausgewählten Objekten verknüpft sind.

Hier wählen Sie Objekte anhand ihres Namens aus, und aus der angezeigten Liste wählen Sie die zu verknüpfenden Objekte aus.

**Hinweis:** Mit SafeGuard PortProtector Domain Partitioning ist die Partitionierung der Gruppen, Organisationseinheiten (OU) und Domänen einer Organisation möglich, so dass darauf nur von den SafeGuard PortProtector Console-Administratoren zugegriffen werden kann, die für deren Bearbeitung verantwortlich sind. Policies, die nicht mit allen Organisationseinheiten in der Domäne des Administrators verknüpft sind, werden im Bereich **Policy mit Organisationsobjekten verknüpfen** des Fensters Policy und in Policy-Abfragen nicht angezeigt und können nicht geändert werden. Wenn jedoch einige der OE, mit denen eine Policy verknüpft ist, in einer Domänenpartition eines Administrators liegen (andere aber nicht), kann die Policy im schreibgeschätzten Modus erscheinen.

**So suchen Sie nach einem bestimmten Objekt:**

1 Geben Sie im Textfeld den Namen des anzuzeigenden Computers oder Benutzers ein. Sie können mehrere Namen durch Komma, Semikolon oder Leerzeichen getrennt eingeben.

2 Markieren Sie das Kontrollkästchen **Exakte Übereinstimmung**, wenn Sie ein Objekt mit einem Namen anzeigen möchten, der genau mit der von Ihnen im Textfeld eingegebenen Zeichenfolge übereinstimmt. Für Computer müssen Sie den vollständigen Computernamen eingeben (einschließlich der Domänenendung). Wenn **Exakte Übereinstimmung** nicht markiert ist, werden im Fenster *Objekt auswählen* Objekte angezeigt, deren Name die von Ihnen eingegebene Zeichenfolge enthält.

3 Wählen Sie aus dem Menü *Objekttyp* unterhalb des Suchfelds Alle die anzuzeigenden Objekttypen aus, oder wählen Sie **Alle**, wenn Sie alle Typen anzeigen möchten.

**Hinweis:** Beim Abfragen zugehöriger Policies enthält das Menü *Objekttyp* nur Computer und Benutzer.

4 Klicken Sie auf **LOS** . Das Fenster zeigt jetzt eine Tabelle der Objekte (eins oder mehrere), deren Name mit Ihren Suchkriterien übereinstimmt. Wenn kein Computer oder Benutzer gefunden wird, dessen Name Ihren Suchkriterien entspricht, ist die Tabelle leer und meldet mit **Keine Ergebnisse gefunden**, dass keine Ergebnisse gefunden wurden.

Die Objekttabelle enthält eine Liste der Objekte, die Ihren Filterkriterien entsprechen. Jede Zeile enthält die folgenden Spalten:

- Kontrollkästchen
- Objektname
- Beschreibung
- Pfad

Sie können die Tabellenansicht folgendermaßen ändern:

- **Sortieren** Sie die Tabelle, indem Sie auf den Spaltentitel der Spalte klicken, nach der Sie sortieren möchten. Klicken Sie nochmals auf die Überschrift, um zwischen auf- und absteigender Reihenfolge zu wechseln. Sie können eine zweite Sortierebene hinzufügen, indem Sie die **Umschalttaste** drücken und auf den zweiten Spaltentitel klicken.
- **Ändern Sie die Spaltenbreite**, indem Sie die Spaltentrennlinien an die gewünschte Stelle ziehen.
- **Verschieben Sie eine Spalte**, indem Sie sie an die gewünschte Position ziehen.

**So verknüpfen Sie eine Policy mit einem Organisationsobjekt:**

**Hinweis:** Die Anleitungen 1-3 in diesem Abschnitt beziehen sich auch auf das Abfragen zugehöriger Policies nach Namen. In diesem Fall werden als Ergebnis Ihrer Auswahl im Fenster *Policies* die Policies angezeigt, die mit den ausgewählten Objekten verknüpft sind.

1. Wählen Sie in der Objekttabelle die Objekte (eins oder mehrere) aus, mit denen Sie die Policy verknüpfen möchten. Markieren Sie dazu die entsprechenden Kontrollkästchen.

2. Um die Objekte der Liste der verknüpften Objekte hinzuzufügen, ohne das Fenster zu schließen, und weitere Objekte über eine zusätzliche Suche hinzuzufügen, klicken Sie auf **Anwenden**.

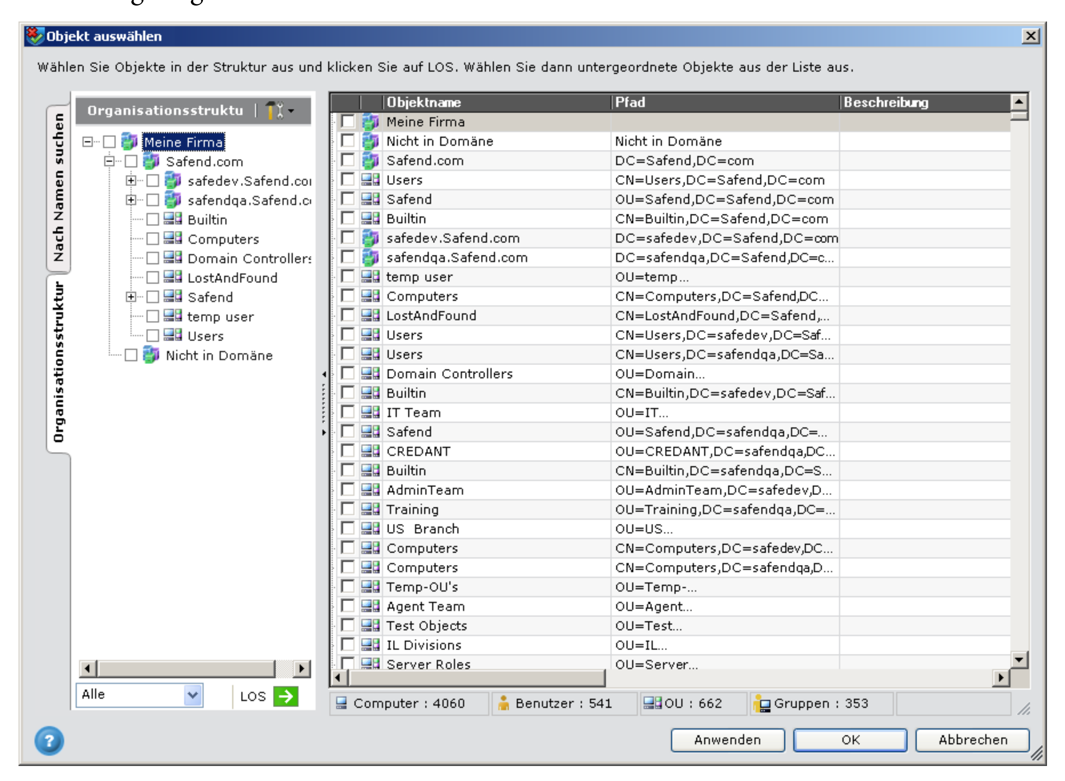
3. Um die Objekte der Liste der verknüpften Objekte hinzuzufügen und das Fenster zu schließen, klicken Sie auf **OK**. Die Objekte werden der Liste hinzugefügt und das Fenster *Objekt auswählen* wird geschlossen. Sie können jetzt eine Liste der verknüpften Objekte im unteren Teil des Fensters *Eigenschaften* sehen.

4. Speichern Sie die Policy. Die Policy wird auf den Clients aktualisiert, wenn die Clients ihre Policy gemäß dem von Ihnen in den Optionen der Policy festgelegten Intervall aktualisieren (siehe *Schritt 17 Optionen definieren* in *Kapitel 3, Definieren von Policies*).

#### 4.2.3.3.2 Filtern von Objekten unter Verwendung der Organisationsstruktur

Die Organisationsstruktur stellt ein weiteres Werkzeug dar, mit dem Sie festlegen können, welche Objekte in der *Objekt*tabelle angezeigt werden sollen. Nachdem Sie diese Objekte ausgewählt und angezeigt haben, können Sie angeben, welche der angezeigten Objekte mit der Policy verknüpft werden sollen.

Die Registerkarte *Organisationsstruktur* zeigt die Domäne(n), Organisationseinheiten, Gruppen, Benutzer und Computer in Ihrer Organisation, sowie die Gruppe Nicht in Domäne (in der alle Computer enthalten sind, die derzeit zu keiner Domäne gehören), wie in der folgenden Abbildung dargestellt:



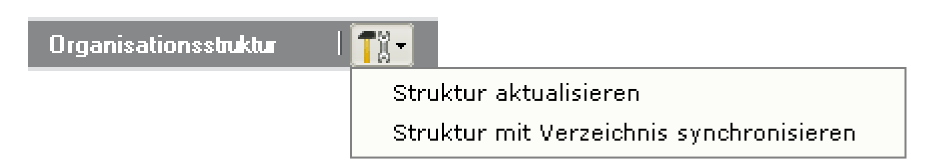
**Hinweis:** Die Organisationsstruktur steht nur dann zur Verfügung, wenn Sie Active Directory oder Novell eDirectory nutzen und die entsprechenden Verzeichnisdefinitionen im Fenster *Administration* festgelegt haben (siehe *Konfigurieren der Einstellungen auf der Registerkarte Allgemein* in *Kapitel 8, Administration*). Wenn Sie keinen dieser Directory-Services nutzen, wird nur eine Gruppe in der Struktur angezeigt: Not In Domain. Durch Auswahl dieser Gruppe werden alle Computer ausgewählt.

###### 4.2.3.3.2.1 Auswählen und Verknüpfen von Objekten aus der Organisationsstruktur

**Hinweis:** Die Anleitungen in diesem Abschnitt beziehen sich auch auf das Abfragen zugehöriger Policies nach Namen. In diesem Fall werden als Ergebnis Ihrer Auswahl im Fenster *Policies* die Policies angezeigt, die mit den ausgewählten Objekten verknüpft sind.

Hier wählen Sie Objekte aus der Organisationsstruktur aus, und aus der angezeigten Liste wählen Sie die zu verknüpfenden Objekte aus.

**Hinweis:** Bevor Sie Ihre Auswahl in der Struktur treffen, möchten Sie sie vielleicht aktualisieren. Sie können die Struktur entweder vom SafeGuard PortProtector Management Server aktualisieren oder sie mit Active Directory/Novell eDirectory synchronisieren, je nachdem, auf welches Directory Sie SafeGuard PortProtector eingestellt haben (das Directory kann aktueller sein, aber es kann auch länger dauern). Die Struktur wird über das Menü Organisationsstruktur (unten dargestellt) aktualisiert, das sich oben in der der Registerkarte Organisationsstruktur befindet.




**So aktualisieren Sie die Organisationsstruktur im Management Server:**

Klicken Sie im Menü **Organisationsstruktur** auf **Struktur aktualisieren**. Die Struktur wird aktualisiert.

**So aktualisieren Sie die Organisationsstruktur im Directory:**

Klicken Sie im Menü **Organisationsstruktur** auf Struktur mit Verzeichnis synchronisieren. Die Struktur wird aktualisiert. Dieser Vorgang kann eine Weile dauern.

**So wählen Sie die gewünschten Organisationseinheiten aus:**

1. Erweitern Sie bei Bedarf die Organisationsstruktur, so dass Organisationseinheiten auf niedrigeren Ebenen angezeigt werden.
2. Wählen Sie die gewünschten Objekte durch Aktivieren der entsprechenden Kontrollkästchen aus.
3. Wählen Sie aus dem Menü *Objekttyp* unterhalb der Organisationsstruktur die anzuzeigenden Objekttypen aus, die Sie für die ausgewählten Objekte anzeigen möchten, oder wählen Sie **Alle**, wenn Sie alle Typen anzeigen möchten. Das bedeutet: Wenn Sie beispielsweise eine bestimmte Organisationseinheit in der Struktur ausgewählt haben, können Sie dann über diese Menüauswahl festlegen, welche Mitglieder der Einheit angezeigt werden sollen (nur Computer, nur Benutzer etc.).

**Hinweis:** Beim Abfragen zugehöriger Policies enthält das Menü *Objekttyp* nur Computer und Benutzer.

4 Klicken Sie unten auf der Registerkarte *Organisationsstruktur* auf **LOS** . Das Fenster zeigt jetzt eine Tabelle mit den ausgewählten Strukturobjekten und allen dazu gehörenden Objekten.

Die Objekttabelle enthält eine Liste der Objekte, die Ihren Filterkriterien entsprechen. Jede Zeile enthält die folgenden Spalten:

- Kontrollkästchen
- Objektname
- Beschreibung
- Pfad

Sie können die Tabellenansicht folgendermaßen ändern:

- **Sortieren** Sie die Tabelle, indem Sie auf den Spaltentitel der Spalte klicken, nach der Sie sortieren möchten. Klicken Sie nochmals auf die Überschrift, um zwischen auf- und absteigender Reihenfolge zu wechseln. Sie können eine zweite Sortierebene hinzufügen, indem Sie die **Umschalttaste** drücken und auf den zweiten Spaltentitel klicken.
- **Ändern Sie die Spaltenbreite**, indem Sie die Spaltentrennlinien an die gewünschte Stelle ziehen.
- **Verschieben Sie eine Spalte**, indem Sie sie an die gewünschte Position ziehen.

**So verknüpfen Sie eine Policy mit einem Organisationsobjekt:**

**Hinweis:** Die Anleitungen 1-3 in diesem Abschnitt beziehen sich auch auf das Abfragen zugehöriger Policies nach Namen. In diesem Fall werden als Ergebnis Ihrer Auswahl im Fenster *Policies* die Policies angezeigt, die mit den ausgewählten Objekten verknüpft sind.

1 Wählen Sie in der Liste der Objekte die Objekte (eins oder mehrere) aus, mit denen Sie die Policy verknüpfen möchten. Markieren Sie dazu die entsprechenden Kontrollkästchen.

2 Um die Objekte der Liste der verknüpften Objekte hinzuzufügen, ohne das Fenster zu schließen, und weitere Objekte über eine zusätzliche Suche hinzuzufügen, klicken Sie auf **Anwenden**.

3 Um die Objekte der Liste der verknüpften Objekte hinzuzufügen und das Fenster zu schließen, klicken Sie auf **OK**. Die Objekte werden der Liste hinzugefügt und das Fenster*Objekt auswählen* wird geschlossen. Sie können jetzt eine Liste der verknüpften Objekte im unteren Teil des Fensters *Eigenschaften* sehen.

4 Optional – Schränken Sie die Policy-Verknüpfung entweder auf Computer oder auf Benutzer innerhalb der selektierten Objekte ein, wie in *Einschränken der Policy auf Benutzer/Computer* beschrieben.

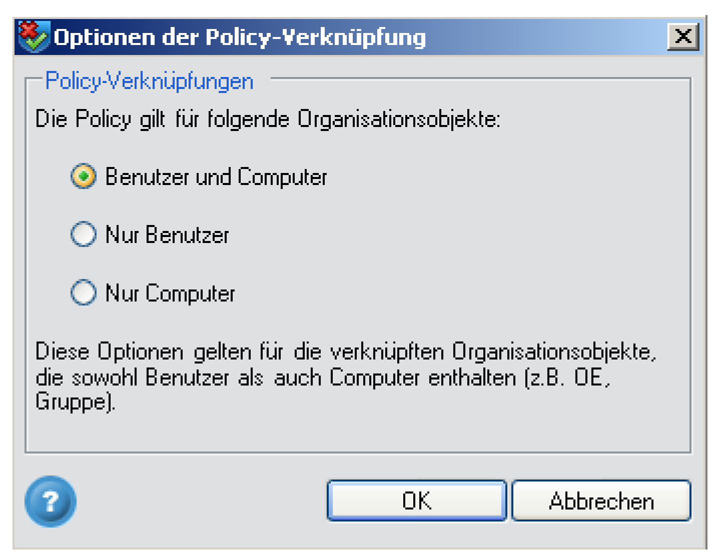
5 Speichern Sie die Policy. Die Policy wird auf den Clients aktualisiert, wenn die Clients ihre Policy gemäß dem von Ihnen in den Optionen der Policy festgelegten Intervall aktualisieren (siehe *Schritt 17 Optionen definieren* im Kapitel *Definieren von Policies*).

### 4.2.4 Einschränken der Policy auf Benutzer/Computer

Mit dem Policy Server lassen sich Policies mit Gruppen, Organisationseinheiten und Domänen sowie mit bestimmten Computern und Benutzern verknüpfen. Wird eine Policy mit Gruppen, Organisationseinheiten und Domänen verknüpft, die sowohl Benutzer als auch Computer enthalten, können Sie die Verknüpfung auf die Computer bzw. Benutzer innerhalb dieses Objekts einschränken. Dies ist normalerweise dann nützlich, wenn Sie eine Computer-Standardpolicy für die gesamte Organisation erstellen. In solchen Fällen wir die Policy mit der gesamten Domäne verknüpft und derart eingeschränkt, dass sie nur für Computer gilt.

**So schränken Sie eine Policy auf Benutzer/Computer ein:**

1 Klicken Sie auf die Schaltfläche **Optionen** rechts neben der Leiste **Policy mit Organisationsobjekten verknüpfen**, um das folgende Fenster anzuzeigen:




2 Wählen Sie die entsprechende Option und klicken Sie auf **OK**.

3 Unten im Bereich **Policy mit Organisationsobjekten verknüpfen** wird jetzt diese Einschränkung angegeben. Er könnte beispielsweise so aussehen: **Diese Policy gilt nur für Benutzer.** Rechts neben dieser Meldung erscheint eine Verknüpfung **Ändern**. Wenn Sie darauf klicken, wird das oben gezeigte Fenster Policy-Verknüpfungen angezeigt.

### 4.2.5 Verknüpfung einer Policy mit Organisationsobjekten lösen

Unter Umständen möchten Sie die Verknüpfung einer Policy mit einem Organisationsobjekt lösen, so dass sie nicht mehr für dieses Objekt gilt.

**Hinweis:** Wenn das Objekt, von dem die Policy gelöst werden soll, geschützt sein muss, stellen Sie sicher, dass ihm eine andere Policy zugeordnet ist.

**So lösen Sie die Verknüpfung einer Policy mit einem Organisationsobjekt:**

1 Wählen Sie im Policy-Fenster *Properties* in der Liste der Objekte, die im Abschnitt Policy mit Organisationsobjekten verknüpfen (untere Hälfte des Fensters) erscheint, das Objekt aus, von dem Sie die Policy lösen möchten.

2 Klicken Sie auf

ODER

Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Löschen** im Kontextmenü.

3 Klicken Sie im daraufhin angezeigten Fenster *Delete Confirmation* auf **Ja**, um das Löschen zu bestätigen. Das Objekt verschwindet aus der Liste der verknüpften Organisationsobjekte.

4 Speichern Sie die Policy.

**Hinweis:** Die Policy gilt weiter für das Objekt mit der gelöschten Verknüpfung, bis Sie die Policy speichern.

## 4.3 Verteilen von SafeGuard PortProtector-Policies unter Verwendung von Active Directory

SafeGuard PortProtector-Policies können mit Hilfe der Microsoft Active Directory GPO-Standardverteilungsfunktion verteilt bzw. veröffentlicht werden. Um diese Funktion nutzen zu können, konfigurieren Sie zunächst das Fenster *Administration* so, dass Active Directory verwenden wird (siehe auch *Veröffentlichungsmethode* im Kapitel *Administration*).

Dies ermöglicht die zentrale Verwaltung der Sicherheitspolicies durch die Systemadministratoren und die automatische Verteilung der Policies an vorhandene Endbenutzer- und Computergruppen. Es brauchen keine Benutzer- und Computergruppen definiert zu werden, und es ist keine spezielle Konfiguration oder Einrichtung erforderlich.

SafeGuard PortProtector legt automatisch jede Policy, die Sie in der SafeGuard PortProtector Management Console definieren, als ein GPO in Active Directory an. Diese Policies werden anschließend automatisch von Active Directory an die Computer und Benutzer verteilt, die zu der Organisationseinheit (OU) gehören, der Sie sie zuweisen.

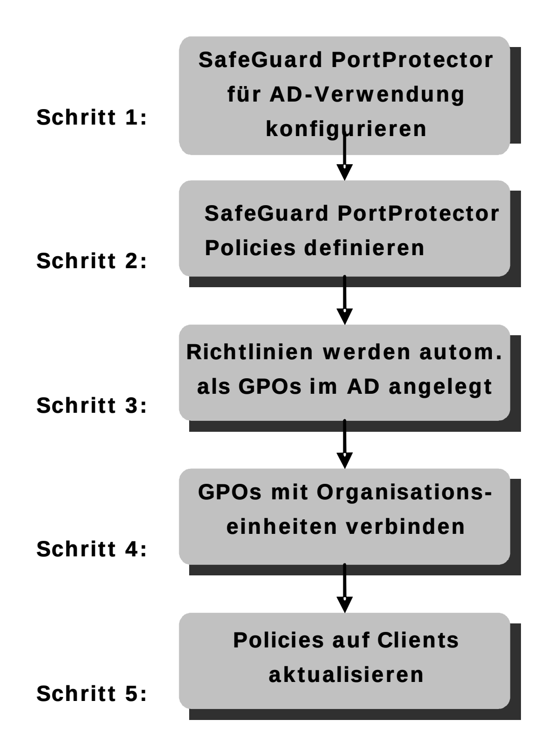
Sie können eine Policy an Ihre gesamte Organisation verteilten, eine andere Policy an die einzelnen Organisationseinheiten, oder jede beliebige, erforderliche Kombination.

Jede Organisationseinheit enthält eine Gruppe von Computern oder Benutzern in der Domäne Ihrer Organisation. Zum Beispiel: die Computer in die Marketing-Abteilung oder der Gruppe der Administratoren. Jeder Computer oder Benutzer kann zu einer einzigen Organisationseinheit gehören. Nachdem Sie eine Policy (GPO) erstellt haben, können Sie sie mit einer Organisationseinheit verknüpfen. Das verknüpfte GPO gilt für alle die Computer und Benutzer, die zu der Organisationseinheit gehören.

Die Policy schützt den Computer nach einem Neustart oder nachdem das definierte GPO-Aktualisierungsintervall abgelaufen ist, das im Active Directory festgelegt wurde. Wenn sich ein geschützter Benutzer am Computer anmeldet, wird die GPO des Benutzers angewendet, d. h., dass eine Benutzer-Policy Vorrang vor einer Computer-Policy hat.

**Hinweis:** Wann immer erforderlich können Sie Policies aktualisieren, ohne auf den standardmäßigen Zeitraum der Policy-Verteilung warten zu müssen (der im Allgemeinen 90 Minuten beträgt). Das kann unter Umständen dann der Fall sein, wenn ein bestimmter Benutzer ein Disk-on-Key-Gerät auf einem bestimmten Computer benutzen muss und nicht warten kann. Das erfolgt problemlos über die SafeGuard PortProtector Management Console in der Clients-Welt mit der Option Update Policy (siehe auch *Aktualisieren einer Policy auf einem Client* in *Kapitel 6, Verwalten von Clients*).

Der folgende Workflow fasst den Vorgang der Policy-Veröffentlichung zusammen.



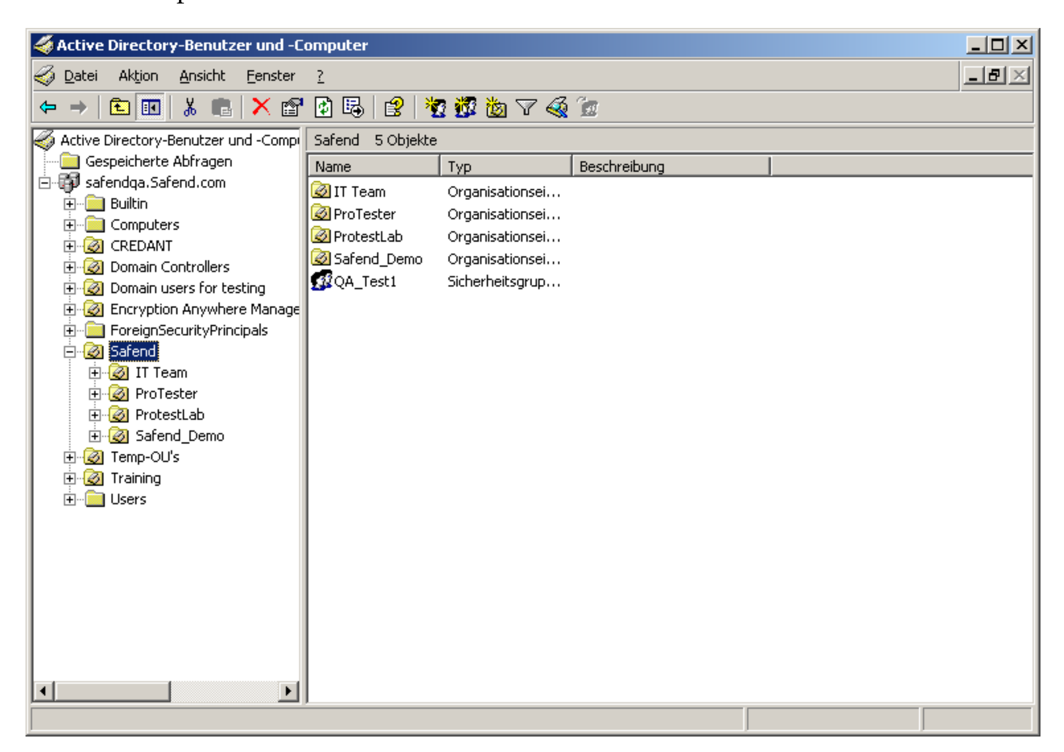

Für diejenigen unter Ihnen, die nicht mit Active Directory vertraut sind, folgt eine Erläuterung darüber, wie GPOs mit Organisationseinheiten verknüpft werden.

### 4.3.1 Verknüpfen von GPOs mit Organisationseinheiten

Dieser Abschnitt ist nur für Benutzer von Active Directory gedacht, die nicht mit dem Verfahren vertraut sind, GPOs mit Organisationseinheiten in Active Directory zu verknüpfen.

**So verknüpfen Sie GPOs mit Organisationseinheiten:**

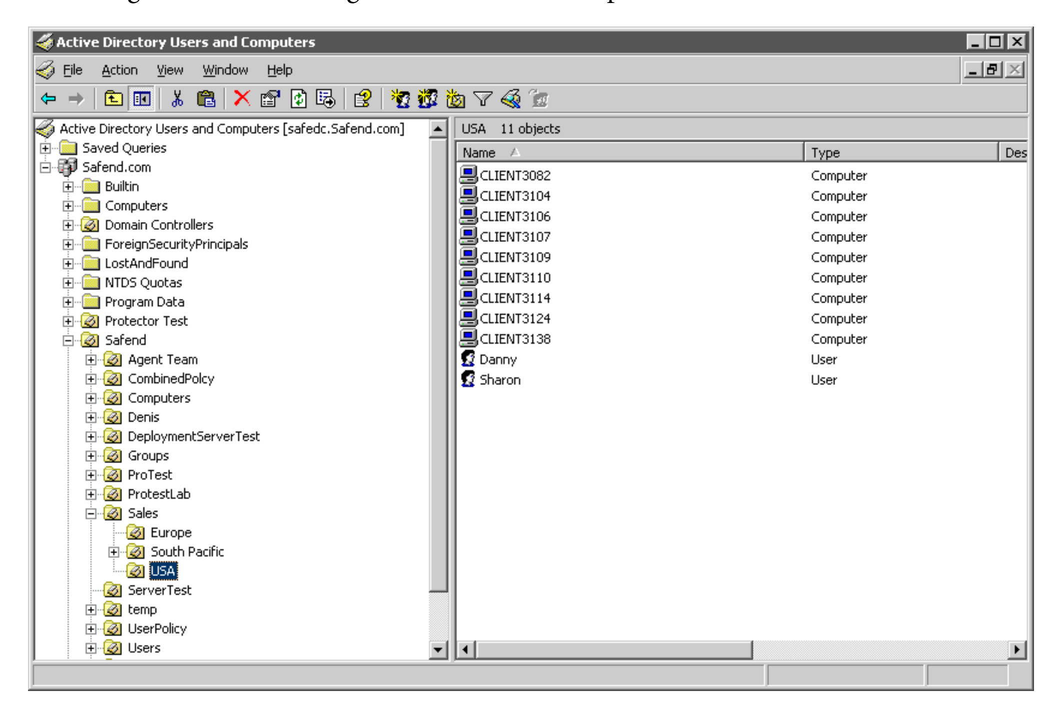
1 Öffnen Sie das Fenster Active Directory Users and Computers, indem Sie **Start | Programme | Administrationswerkzeuge | Active Directory Users and Computers** wählen. Hier ein Beispiel:



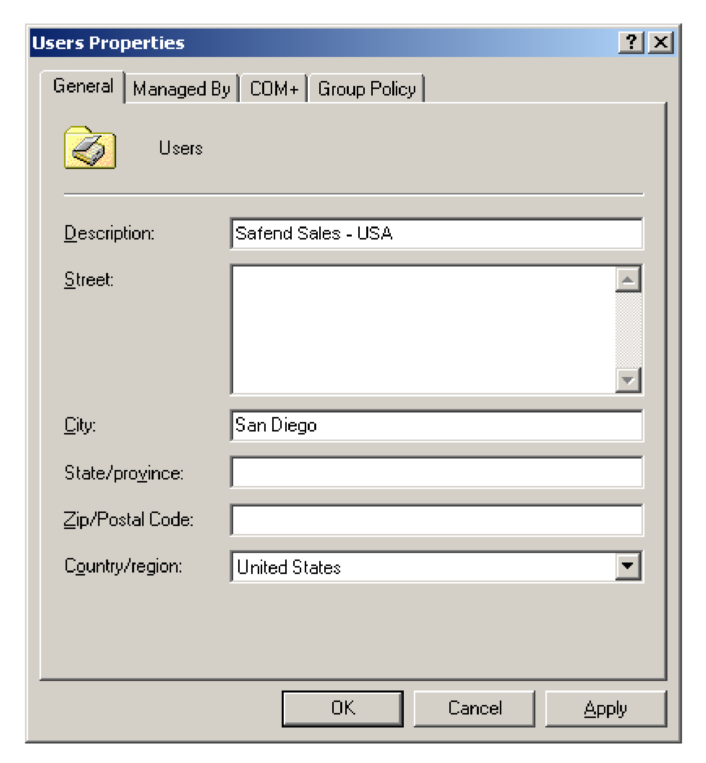

Dieses Beispielfenster zeigt die Domäne und den Pfad, in dem die GPOs in Active Directory gespeichert sind. Bei der Installation von SafeGuard PortProtector entdeckt das System automatisch die Domäne, zu der der Computer gehört, und legt dann unter dieser Domäne GPOs an.

Die Organisationseinheiten in diesem Active Directory erscheinen als Ordner oder Unterordner und dem Zweig. Zum Beispiel: Sales, wie oben gezeigt. Dabei handelt es sich um die Organisationseinheiten, an die SafeGuard PortProtector-Policies verteilt werden.

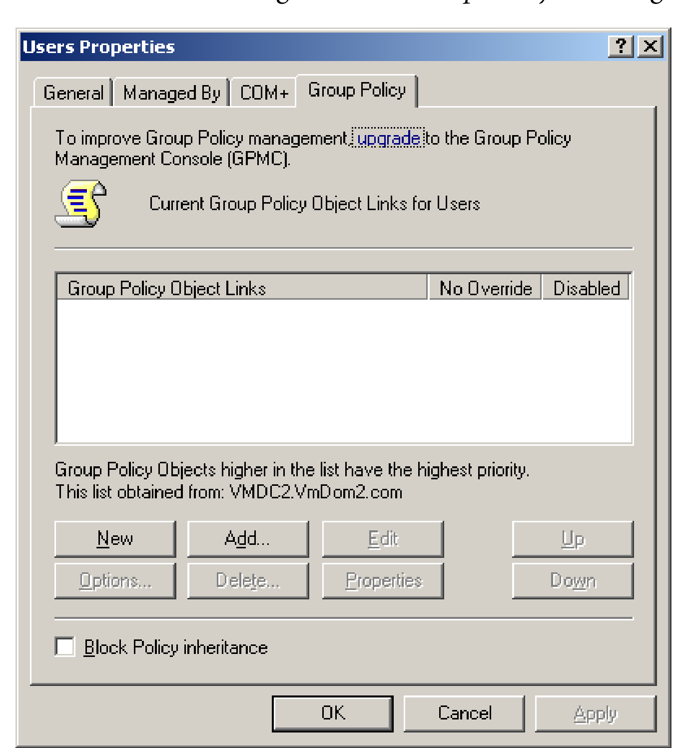
Wählen Sie einen Ordner aus, um eine Liste der Computer und Benutzer anzuzeigen, die zu einer Organisationseinheit gehören. Hier ein Beispiel:



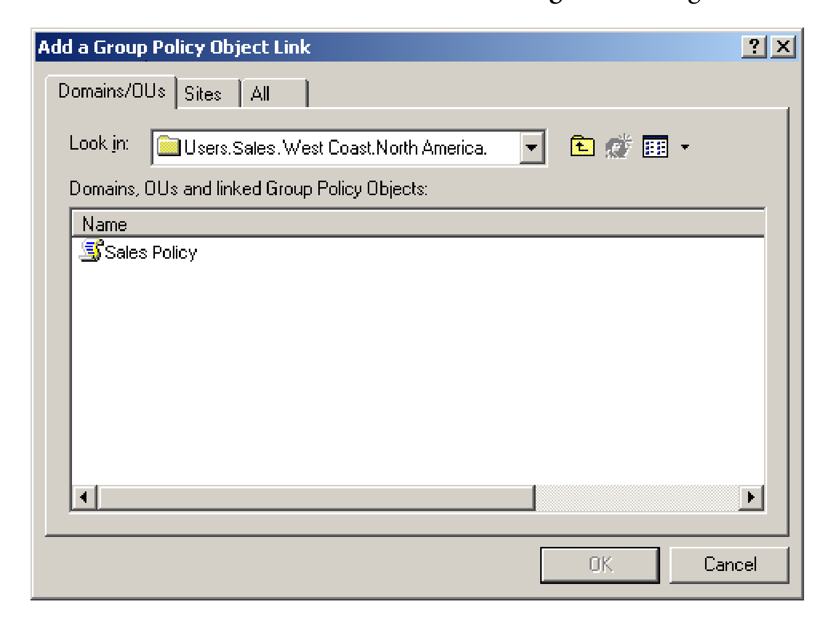

2 Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, mit der Sie ein GPO verknüpfen möchten, und wählen Sie **Properties**. Das folgende Fenster wird angezeigt:



3 Wählen Sie die Registerkarte *Group Policy*. Das folgende Fenster wird angezeigt:




4 Klicken Sie auf die Schaltfläche **Hinzufügen**. Das folgende Fenster wird angezeigt:




In diesem Fenster werden alle GPOs aufgeführt, die derzeit mit dieser Organisationseinheit verknüpft sind.

5 Wählen Sie in diesem Fenster die Registerkarte **Alle**. Es wird eine alphabetische Liste der GPOs angezeigt.

6 Wählen Sie aus der Liste die Policy (GPO) aus, die Sie dieser Organisationseinheit hinzufügen möchten, und klicken Sie auf **OK**. Sobald Sie eine Policy ausgewählt haben, wird sie im Fenster *OU Properties* auf der Registerkarte *Group Policy* und in der Organisationsstruktur im Fenster *Active Directory Users and Computers* angezeigt. Wiederholen Sie diesen Vorgang für jede dieser Organisationseinheit hinzuzufügende Policy.

7 Klicken Sie auf **OK**. Diese Policies werden dann automatisch an die Organisationseinheiten (Computer und Benutzer) verteilt, denen Sie sie zugewiesen haben. In *Policy aktualisiert* im Kapitel *Endbenutzer-Erfahrung* finden Sie eine Beschreibung der Endbenutzer-Erfahrung bei der Verteilung einer neuen Policy.

#### 4.3.1.1 Anwenden von Policies pro Sicherheitsgruppe

Normalerweise werden SafeGuard PortProtector-Policies (GPOs) auf Objekte angewandt, die sich in einem OU-Container (Computer oder Benutzer) befinden. Bei einigen großen Organisationen ist die Verwaltung unter Umständen mühsam und schwierig. Eine andere Möglichkeit besteht darin, die Policy bei Benutzern anzuwenden, die sich in Sicherheitsgruppen befinden. Hierfür wird ein so genanntes Sicherheitsfilterungsverfahren genutzt.

Ein gutes Beispiel für eine Organisation, die dieses Verfahren einsetzen könnte, ist eine Organisation bei der alle Benutzer in einer Organisationseinheit und alle Computer in einer anderen Organisationseinheit (in der Domäne) enthalten sind.

In diesem Fall wäre es einfacher, die vorhandenen Sicherheitsgruppen zu nutzen und die Policy darauf anzuwenden, satt die Computer/Benutzer in einer neuen OU-Struktur anzuordnen.

Die Sicherheitsfilterung ist im Wesentlichen ein Verfahren, bei dem Sie mehrere GPOs auf dieselbe Organisationseinheit (die Benutzer enthält) anwenden und dann die ACE (Access Control Entries, Zugangssteuerungseinträge) bei den GPOs ändern, so dass nur Benutzer in bestimmten Sicherheitsgruppen zum Lesen berechtigt sind, und diese spezifische Protector-/Gruppenpolicy anwenden.

ACE-Standardeinträge für ein neues Group Policy Object (GPO):

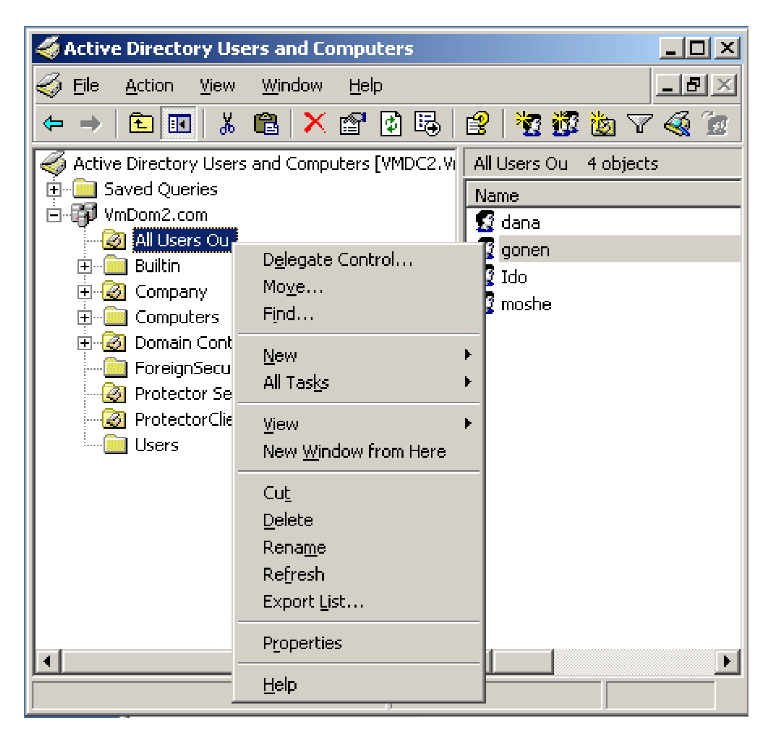
| Security Principal | Read | Gruppen-Policy anwenden |
|---|---|---|
| **Authenticated users** | Allow | Allow |
| **Creator owner** | Allow (implicit) | |
| **Domain admins** | Allow | |
| **Enterprise admins** | Allow | |
| **Enterprise domain controllers** | Allow | |
| **System** | Allow | |

Um die Sicherheitsfilterung anwenden zu können, müssen die gewünschten SafeGuard PortProtector-Policies erstellt und als GPOs in Active Directory gespeichert werden, wie wir es in jedem Falle täten. Diese neuen Policies müssen mit der Organisationseinheit verknüpft werden, die alle Benutzer enthält.

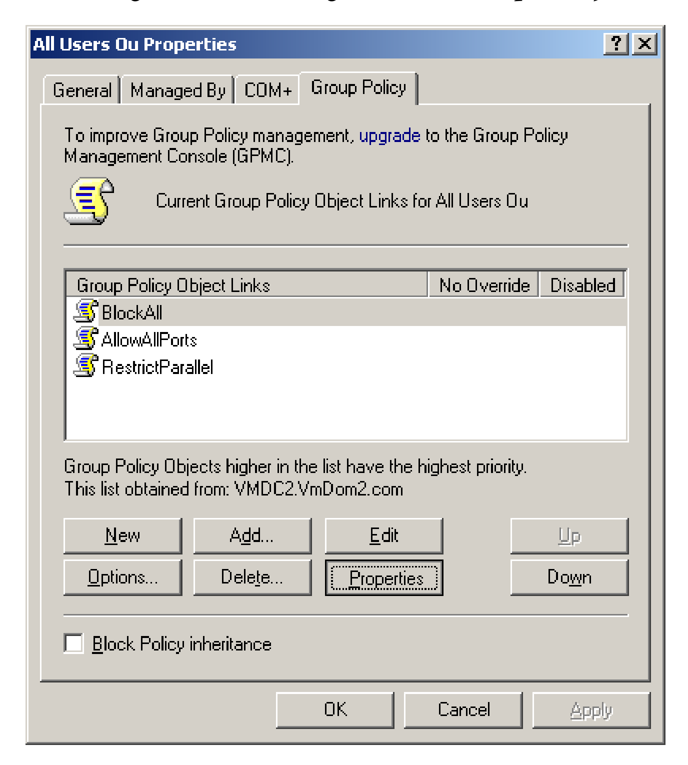
Zum Beispiel könnte eine Policy, die zum Blockieren aller Ports erstellt wurde (namens BlockAll) auf alle Benutzer angewandt werden, die sich in einer Sicherheitsgruppe namens BlockAll befinden.

**So ändern Sie die ACE in der BlockAll-Policy:**

1 Öffnen Sie das Fenster *Active Directory Users and Computers*, klicken Sie mit der rechten Maustaste auf die OU, die alle Benutzer enthält, und wählen Sie "**Properties**".

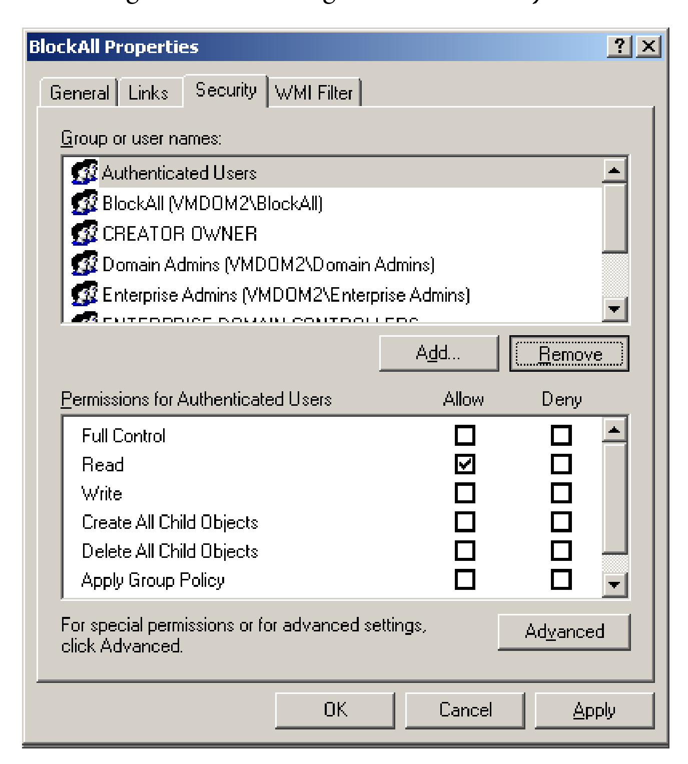



2 Navigieren Sie zur Registerkarte ***Group Policy***:



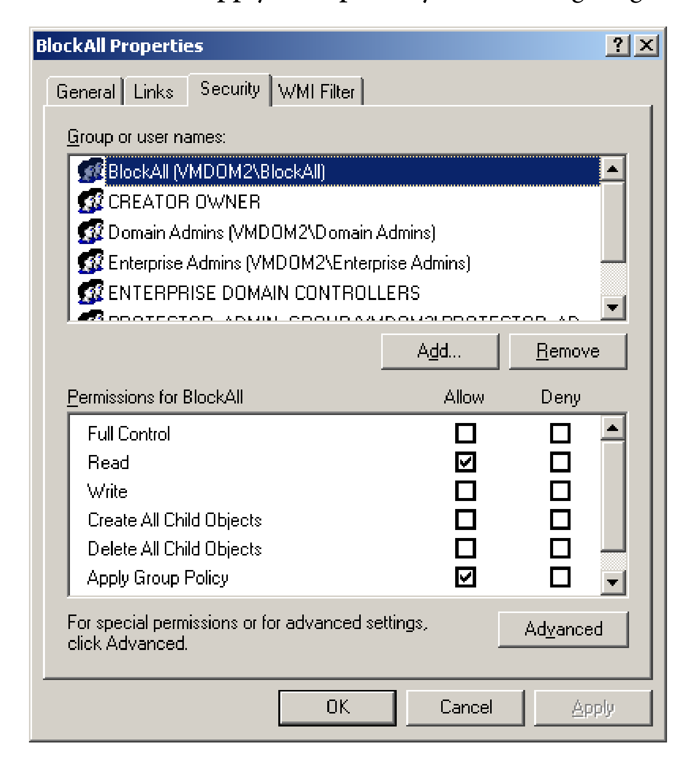

3 Wählen Sie die BlockAll-Policy und klicken Sie auf **Properties.**

4 Navigieren Sie zur Registerkarte ***Security***:




5 Entfernen Sie *Authenticated Users* aus dem ACE.

6 Fügen Sie die Sicherheitsgruppe BlockAll hinzu und verleihen Sie ihr die Berechtigungen **Read** und **Apply Group Policy**, wie unten gezeigt:




7 Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern.

## 4.4 Verteilen von SafeGuard PortProtector-Policies unter Verwendung von Registry-Dateien

Mit Hilfe der Registry-Dateien können Sie andere Managementanwendungen zur Verteilung von Policies einsetzen, wenn Sie den Policy Server oder den Active Directory GPO-Mechanismus nicht verwenden möchten oder nicht über die erforderliche Infrastruktur verfügen.

Diese Option speichert Registry-Dateien in einem freigegebenen Ordner und ermöglicht es Ihnen, SafeGuard PortProtector-Policies mit Hilfe von Drittanbieter-Tools an die SafeGuard PortProtector Clients zu verteilen. Wenn diese Option genutzt wird, erzeugt SafeGuard PortProtector zwei Kopien von der Registry-Datei, von denen eine für Computer (zum Beispiel **MyPolicy(MACHINE).reg**) und eine für Benutzer (zum Beispiel namens **MyPolicy(USER).reg**) geeignet ist.

**So verteilen Sie eine Policy an einen Client unter Verwendung von .reg-Dateien:**

1. Doppelklicken Sie auf die gewünschte .reg-Datei und im Bestätigungsfenster auf **Ja**, um deren Daten zur Registry hinzuzufügen.
2. Aktualisieren Sie die Policy auf dem Client, wie in *Aktualisieren der Client-Policy* im Kapitel *Endbenutzer-Erfahrung* erläutert.

In vielen Fällen möchten Sie vielleicht. den Vorgang, bei dem Policies durch ein Fremdtool verteilt werden (wie etwa SMS, Novell eDirectory), nach dem Bearbeiten/Erstellen von Policies automatisieren. Weitere Informationen finden Sie in *Ausführbare Datei nach Veröffentlichung* **ausführen** im *Kapitel Administration*.

## 4.5 Zusammenführen von Policies

Wenn mehrere Policies mit einem Organisationsobjekt verknüpft sind, können die Definitionen aller verknüpften Policies zusammengeführt werden, um so die Definitionen zu produzieren, die auf dem Endpunkt durchgesetzt werden. Ein typisches Beispiel für diese Fähigkeit ist das Erstellen einer allgemeinen Policy für eine bestimmte Abteilung, und einer weiteren Policy für einen bestimmten Benutzer in dieser Abteilung, der zusätzliche Berechtigungen benötigt. Je nachdem, welche der gewählten Policy-Verteilungsmethode ausgewählt wird, kann das Zusammenführen wie folgt erfolgen:

**Unter Verwendung von Policy Server –** Das Zusammenführen von Policies erfolgt automatisch.

**Unter Verwendung von Active Directory –** Das Zusammenführen von Policies ist optional und wird in *Konfigurieren der Einstellungen auf der Registerkarte Policies* im Kapitel *Administration*, definiert.

**Unter Verwendung von Registry-Dateien –** Das Zusammenführen von Policies ist nicht möglich.

Das Zusammenführen von Policies funktioniert folgendermaßen:

- **Berechtigungen**: für jede/n/s Port/Gerät/Speichergerät/Dateityp/WiFi-Link wird aus allen zusammengeführten Policies die Definition mit den meisten Berechtigungen angewandt (eine Erläuterung der Reihenfolge der Berechtigungen finden Sie in *Speicherkontrolle – Registerkarte Weiße Liste* im Kapitel *Definieren von Policies*). Es gibt jedoch ein paar Ausnahmen zu dieser **mit meisten Berechtigungen anwenden**-Regel, die im Folgenden angegeben werden.
- **Einstellungen**: Für jeden Einstellungstyp (Protokollierung, Alarme etc.) werden die Definitionen aus der Policy übernommen, deren Name in alphabetischer Reihenfolge zuerst kommt.

**Hinweis:** Beim Zusammenführen von Policies wird empfohlen, dass Sie die allgemeinen Policy-Einstellungen statt policy-spezifischer Einstellungen verwenden, um eine Fehlkonfigurierung der Policy-Einstellungen zu vermeiden, die nur aus einer Policy übernommen werden.

**Beispiel 1**:

Die zusammengeführten Policies sind PolicyA und PolicyB:

Die Berechtigung für Wechselspeichergeräte in PolicyA ist **Zulassen**.

Die Berechtigung für Wechselspeichergeräte in PolicyB ist **Verschlüsseln**.

PolicyA und PolicyB verfügen über verschiedene Einstellungen.

Werden nun PolicyA und PolicyB auf einem Endpunkt zusammengeführt, wird die Berechtigung **Zulassen** für Wechselspeichergeräte übernommen, weil die Berechtigung **Zulassen** höher ist als **Verschlüsseln**.

Da PolicyA und PolicyB über verschiedene Einstellungen verfügen, werden die Einstellungen von den Definitionen in PolicyA übernommen, weil sie in alphabetischer Reihenfolge zuerst steht.

Beispiel 2:

Die zusammengeführten Policies sind PolicyA und PolicyB:

Die Berechtigung für Wechselspeichergeräte in PolicyA ist **Zulassen**.

Die Berechtigung für Wechselspeichergeräte in PolicyB ist **Schreibgeschützt**.

Werden nun PolicyA und PolicyB auf einem Endpunkt zusammengeführt, wird die Berechtigung **Zulassen** für Wechselspeichergeräte übernommen, weil die Berechtigung **Zulassen** höher ist als **Schreibgeschützt.**

Beispiel 3:

Die zusammengeführten Policies sind PolicyA und PolicyB:

Die Berechtigung für die Disk-on-Key Smart-Funktionalität in PolicyA ist **Zulassen**.

Die Berechtigung für Wechselspeichergeräte in PolicyB ist **Sperren**.

Werden nun PolicyA und PolicyB auf einem Endpunkt zusammengeführt, wird die Berechtigung **Zulassen** für die Disk-on-Key Smart-Funktionalität übernommen, weil die Berechtigung **Zulassen** höher ist als **Sperren**.

Beispiel 4:

Die zusammengeführten Policies sind PolicyA und PolicyB:

Die Berechtigung für die Disk-on-Key Smart-Funktionalität in PolicyA ist **Zulassen**.

Die Berechtigung für Wechselspeichergeräte in PolicyB ist **Sperren**.

Werden nun PolicyA und PolicyB auf einem Endpunkt zusammengeführt, wird die Berechtigung **Zulassen** für die Disk-on-Key Smart-Funktionalität übernommen, weil die Berechtigung **Zulassen** höher ist als **Sperren**.

**Hinweis:** Wenn Policies auf einem Client zusammengeführt werden, werden die Namen aller zusammengeführten Policies in den Logs dieses Clients und die Daten in der Clients Table angezeigt.

## 4.5.1 Zusammenführen von Policies bei nicht klassifizierten, zugelassenen Geräten

Wenn nicht klassifizierte Geräte als **Zugelassen** auf der Seite *Policies* im Fenster *Administration* definiert sind (siehe auch Beschreibung in *Zulassen/Sperren nicht klassifizierter Geräte*), verhält sich das Zusammenführen von Policies bezüglich der Gerätekontrolle anders.

In diesem Fall werden die Gerätekontrolldefinitionen mit den geringsten Berechtigungen aller zusammengeführten Policies durchgesetzt. Das bedeutet, dass die auf der Registerkarte **Gerätekontrolle** der Policy definierten Sicherheitsaktionen so zusammengeführt werden, dass die mit den geringsten Berechtigungen in Kraft treten, während die übrigen Policy-Definitionen (wie etwa Portkontrolle, Speicherkontrolle und Dateitypkontrolle) weiter so zusammengeführt werden, dass die Sicherheitsaktionen mit den meisten Berechtigungen wirksam werden (siehe Beschreibung weiter oben).

Auf diese Weise kann der Administrator während der Einführung von SafeGuard PortProtector in der Organisation die Geräte sukzessive in verschiedenen Bereichen der Organisation einschränken, so wie SafeGuard PortProtector in der Organisation eingeführt wird.

**Hinweis:** Wenn nicht klassifizierte Geräte als **Zugelassen** auf der Seite *Policies* im Fenster *Administration* definiert werden, wird dadurch das Fenster *Gerätekontrolle* auf der Registerkarte *Allgemein* des Fensters *Policy* beeinflusst. Das Fenster *Gerätekontrolle* zeigt **Zulassen** ( ) im Bereich **Devices Not Approved in Device Types or White List** für *Nicht klassifizierte Geräte Devices* unten im Fenster. Hierdurch wird gekennzeichnet, dass nicht klassifizierte Geräte zugelassen werden, und dass die Gerätekontrolle der Policy-Zusammenführung wie oben beschrieben beeinflusst wurde.

**Beispiel**:

Das folgende Beispiel zeigt, wie sich Gerätekontrolle und Speicherkontrolle verhalten, wenn nicht klassifizierte Geräte als **Zugelassen** auf der Seite *Policies* im Fenster *Administration* definiert sind.

Die zusammengeführten Policies sind PolicyA und PolicyB:

In PolicyA gibt die Gerätekontrolle an, dass Drucker zugelassen sind.

In PolicyA gibt die Speicherkontrolle an, dass Wechselspeichergeräte zugelassen sind.

In PolicyB gibt die Gerätekontrolle an, dass Drucker gesperrt sind.

In PolicyB gibt die Speicherkontrolle an, dass Wechselspeichergeräte gesperrt sind.

Wenn PolicyA und PolicyB für einen bestimmten Endpunkt zusammengeführt werden, dann werden die Drucker gesperrt, weil die Sicherheitsaktion der Gerätekontrolle mit den geringsten Berechtigungen wirksam wird und 'sperren' einschränkender ist als 'zulassen'.

Wechselspeichergeräte werden zugelassen, weil die Sicherheitsaktion der Speicherkontrolle mit den meisten Berechtigungen wirksam wird und 'zulassen' mehr Berechtigungen bietet als 'sperren' (da die Sicherheitsaktionen der Wechselspeichergeräte Definitionen der Speicherkotrolle und nicht Definitionen der Gerätekontrolle sind, werden sie weiterhin standardmäßig, d. h. mit den meisten Berechtigungen, zusammengeführt).

## 4.5.2 Zusammenführen von Policies bei anderen zugelassenen Dateitypen

Wenn **Andere Dateitypen** als **Zulassen** auf der Registerkarte **Dateitypkontrolle** der Policy definiert sind, verhält sich das Zusammenführen von Policies bezüglich der Dateikontrolle anders.

In diesem Fall werden die Dateitypkontrolldefinitionen mit den geringsten Berechtigungen aller zusammengeführten Policies durchgesetzt. Das bedeutet, dass die auf der Registerkarte **Dateitypkontrolle** der Policy definierten Sicherheitsaktionen so zusammengeführt werden, dass die mit den geringsten Berechtigungen in Kraft treten, während die übrigen Policy-Definitionen (wie etwa Port Control, Device Control, Storage Control und WiFi Control) weiter so zusammengeführt werden, dass die Sicherheitsaktionen mit den meisten Berechtigungen wirksam werden, wie oben beschrieben.

**Beispiel:**

PolicyA und PolicyB sind zwei zusammengeführte Policies.

PolicyA gibt an, dass die Berechtigung für das Schreiben für Other File Types auf **Gesperrt** und für das Schreiben für Dateityp Published Documents auf **Gesperrt** gesetzt ist.

PolicyB gibt an, dass die Berechtigung für das Schreiben für Other File Types auf **Gesperrt** und für das Schreiben für File Type Published Documents auf **Zugelassen** gesetzt ist.

Wenn PolicyA und PolicyB auf einem Endpunkt zusammengeführt werden, findet die Berechtigung **Zugelassen** für Published Document Anwendung, weilAndere Dateitypen auf **Gesperrt** gesetzt ist. Auf diese Weise wird die Definition mit den meisten Berechtigungen für Dateigruppen, inklusive Published Documents, angewendet.

# 5 Anzeigen von Logs

## Über dieses Kapitel

Dieses Kapitel beschreibt die Logs-Welt, in der Sie SafeGuard PortProtector-Logs und Shadow-Dateien anzeigen, verwalten und erfassen sowie einige administrative Aufgaben ausführen können. Das Kapitel enthält die folgenden Abschnitte:

- ***Übersicht*** beschreibt Logs sowie deren Funktion und liefert einen kurzen Überblick über die Logs-Welt.
- ***Kurze Übersicht über die Logs-Welt*** beschreibt das Hauptfenster der Logs-Welt.
- ***Log-Tabelle*** beschreibt die Log-Tabelle und ihren Inhalt, und erläutert, wie Sie sie verwalten und darin navigieren können.
- ***Filtern nach Herkunft des Logdatensatzes*** beschreibt, wie Sie die Log-Tabelle so filtern können, dass nur Logs für ausgewählte Organisationseinheiten, Computer oder Benutzer angezeigt werden.
- ***Abfragen*** beschreibt die Abfragen, die eine weitere Methode zur Filterung der Log-Tabelle darstellen.
- ***Optionen für aktives Fenster*** behandelt das Duplizieren, Lösen und Schließen eines Fensters.
- ***Erfassen von*** Logs beschreibt, wie Sie Logs jederzeit erfassen können, ohne auf den Ablauf des Logerfassungsintervalls warten zu müssen.
- ***Verfolgen des Fortschritts von Client-Tasks*** beschreibt, wie der Fortschritt von Client-Tasks, wie etwa Logerfassung und Policy-Aktualisierung, verfolgt werden.
- ***Struktur der Log-Tabellen*** beschreibt den Aufbau der Client-, Datei- und Server-Logtabellen.

## 5.1 Übersicht

Ereignisse, die auf durch SafeGuard PortProtector Clients geschützten Endpunkten auftreten, werden in Logs bzw. Alarmen aufgezeichnet. Bei einem Ereignis kann es sich um das Anschließen oder Abnehmen eines Geräts, die Verbindung zu einem kabellosen Netz, Manipulationsversuche oder Administrator-Anmeldung etc. handeln. Diese Ereignisse werden als Client-Logs gespeichert. Logs/Alarme, die den Namen einer Datei aufzeichnen, die von einem Speichergerät gelesen oder darauf geschrieben wird, werden als File-Logs gespeichert.

Die Logs und Alarme von Client- und Dateiprotokollierung können sich auf einen Computer oder einen Benutzer beziehen, je nachdem, wie die vorgebende Policy angewandt ist.

Zusätzlich zu den Ereignissen, die auf geschützten Endpunkten auftreten, werden Logs und Alarme auch durch SafeGuard PortProtector Management Server-Ereignisse erzeugt, wie etwa Anmeldung eines Administrators, Veröffentlichen von Policies und Ausführen von Datensicherungen.

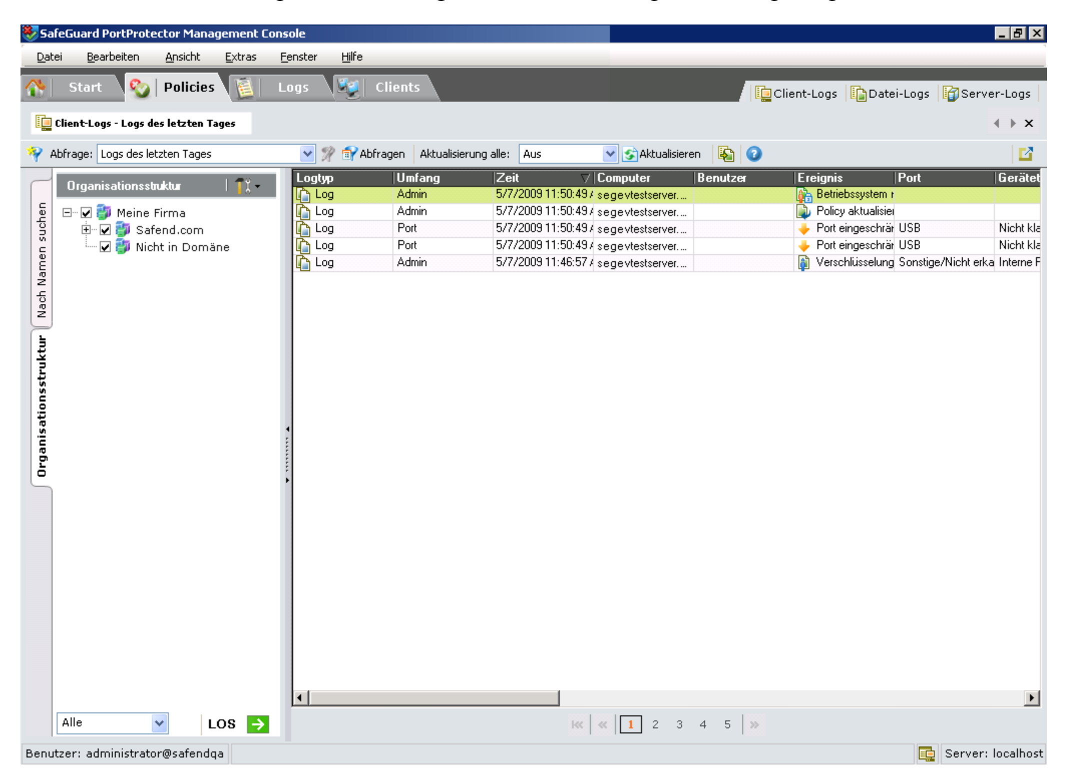
Client- und Server-Logs und -Alarme werden in Intervallen, die in der Policy des Clients definiert sind, an einen Logspeicher auf dem Management Server gesendet und dort gespeichert. Wenn nötig können sie auch vom Administrator zu einem anderen Zeitpunkt erfasst werden. Dieses Kapitel beschreibt die Logs-Welt, die verschiedene Möglichkeiten zur Abfrage und Anzeige von Logs und Alarmen bietet.

## 5.2 Kurze Übersicht über die Logs-Welt

Diese Übersicht bezieht sich auf Client-Logs und File-Logs. Die Fenster des Server-Logs unterscheiden sich dadurch, dass sie keinen Abschnitt der Organisationsstruktur haben.

**So öffnen Sie die Logs-Welt:**

Klicken Sie auf die Registerkarte **Logs**. Das Fenster Logs wird angezeigt:



Das Fenster der Logs-Welt enthält die Abschnitte und Steuerungsschaltflächen, die in *Übersicht über die Anwendung* im Kapitel *Erste Schritte*, beschrieben wurden. Die Startschaltflächen und einige der Menüoptionen sind speziell für die Logs-Welt.

## 5.2.1 Startschaltflächen

Die spezifischen Startschaltflächen in der Logs-Welt sind:

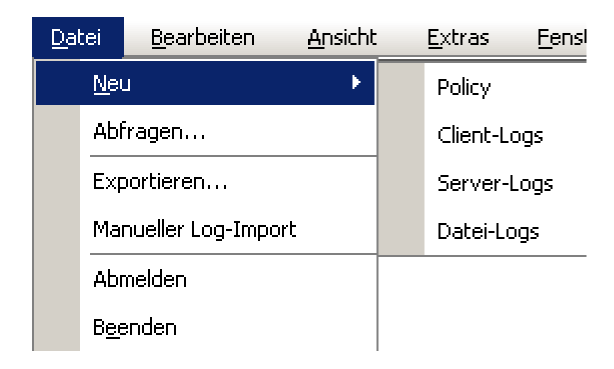
- **Client-Logs** – Wenn Sie auf diese Schaltfläche klicken, wird ein neues Fenster Client Logs für die aktuelle Auswahl in der Organisationsstruktur angezeigt (eine Erläuterung der Organisationsstruktur finden Sie in *Filtern nach Herkunft des Logdatensatzes*).
- **File-Logs** – Wenn Sie auf diese Schaltfläche klicken, wird ein neues Fenster File Logs für die aktuelle Auswahl in der Organisationsstruktur angezeigt (eine Erläuterung der Organisationsstruktur finden Sie in *Filtern nach Herkunft des Logdatensatzes*).
- **Server-Logs** – Wenn Sie auf diese Schaltfläche klicken, wird ein neues Fenster Server Logs mit den Server-Logs angezeigt. Eine Beschreibung zu Client-, File- und Server-Logs finden Sie in *Log-Tabelle*.

## 5.2.2 Menüs

Einige der Menüoptionen in der Logs-Welt sind speziell für diese Welt. Nachstehend finden Sie eine Beschreibung der einzelnen Menüs und der Optionen.

### 5.2.2.1 Menü Datei

Im Menü *Datei* in der Logs-Welt können Sie andere Welt-Fenster öffnen, Abfragen verwalten, Abfragen exportieren etc.



Das Menü *Datei* enthält in der Logs-Welt folgende Optionen:

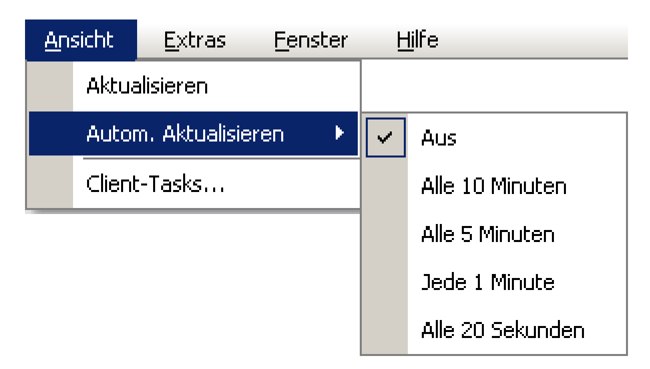
| Option | Beschreibung |
|---|---|
| **Neu** | Öffnet ein Untermenü, über das Sie ein neues Policy-, ein neues Client Log-, ein neues Server Log- oder ein neues File Log-Fenster öffnen können. |
| **Abfragen** | Ermöglicht Ihnen das Verwalten der Abfragen. |
| **Exportieren** | Exportiert die Abfrage in eine externe Datei. |
| **Manueller Log-Import** | Ermöglicht es Ihnen, Ihre Log-Dateien in organisierter Form zu speichern. Sie können entweder *Bestimmte Dateien importieren* oder *Logs aus Ordner importieren*. |
| **Benutzerrolle ändern** | Einem SafeGuard PortProtector-Administrator können mehrere Rollen zugewiesen werden, um die verschiedenen Domänenpartitionen zu definieren, für die er verantwortlich ist. Nachdem sich ein solcher Administrator angemeldet hat, wird automatisch ein Auswahlfenster angezeigt, in dem er die entsprechende Rolle für seine Arbeit auswählen kann.<br><br>**Anmerkung:** Eine Benutzerrolle definiert die Funktionen, Organisationseinheiten und Domänen einer Organisation, auf die ein SafeGuard PortProtector-Administrator zugreifen kann (siehe auch *Definieren von Rollen*).<br><br>Über die Option **Benutzerrolle ändern** kann ein solcher Administrator von dieser Rolle jederzeit zu einer anderen, ihm zugewiesenen Rolle wechseln. |
| **Abmelden** | Meldet den aktuellen Benutzer von der Management Console ab. |
| **Beenden** | Meldet den aktuellen Benutzer ab und schließt die SafeGuard PortProtector Management Console. |

### 5.2.2.2 Menü Bearbeiten

Das Menü *Bearbeiten* ist in der Logs-Welt deaktiviert.

### 5.2.2.3 Menü Ansicht

Über das Menü *Ansicht* können Sie das Fenster *Logs* aktualisieren, das eine Liste Ihrer Logs anzeigt, und den Fortschritt von Client-Tasks anzeigen lassen.




Das Menü *Ansicht* enthält folgende Optionen:

| Option | Beschreibung |
|---|---|
| **Aktualisieren** | Aktualisiert das Log, so dass es auf dem neuesten Stand ist. |
| **Autom. Aktualisieren** | Öffnet ein Untermenü, über das Sie festlegen können, wie häufig der aktive Logtyp (*Client*, *File* oder *Server*) automatisch aktualisiert werden soll. |
| **Client-Tasks** | Zeigt den Verlauf der Client-Tasks. |

### 5.2.2.4 Menü Extras

Das Menü *Extras*, das bei allen Welten gleich ist, ist in *Menü* im Kapitel *Erste Schritte*, beschrieben.

### 5.2.2.5 Menü Fenster

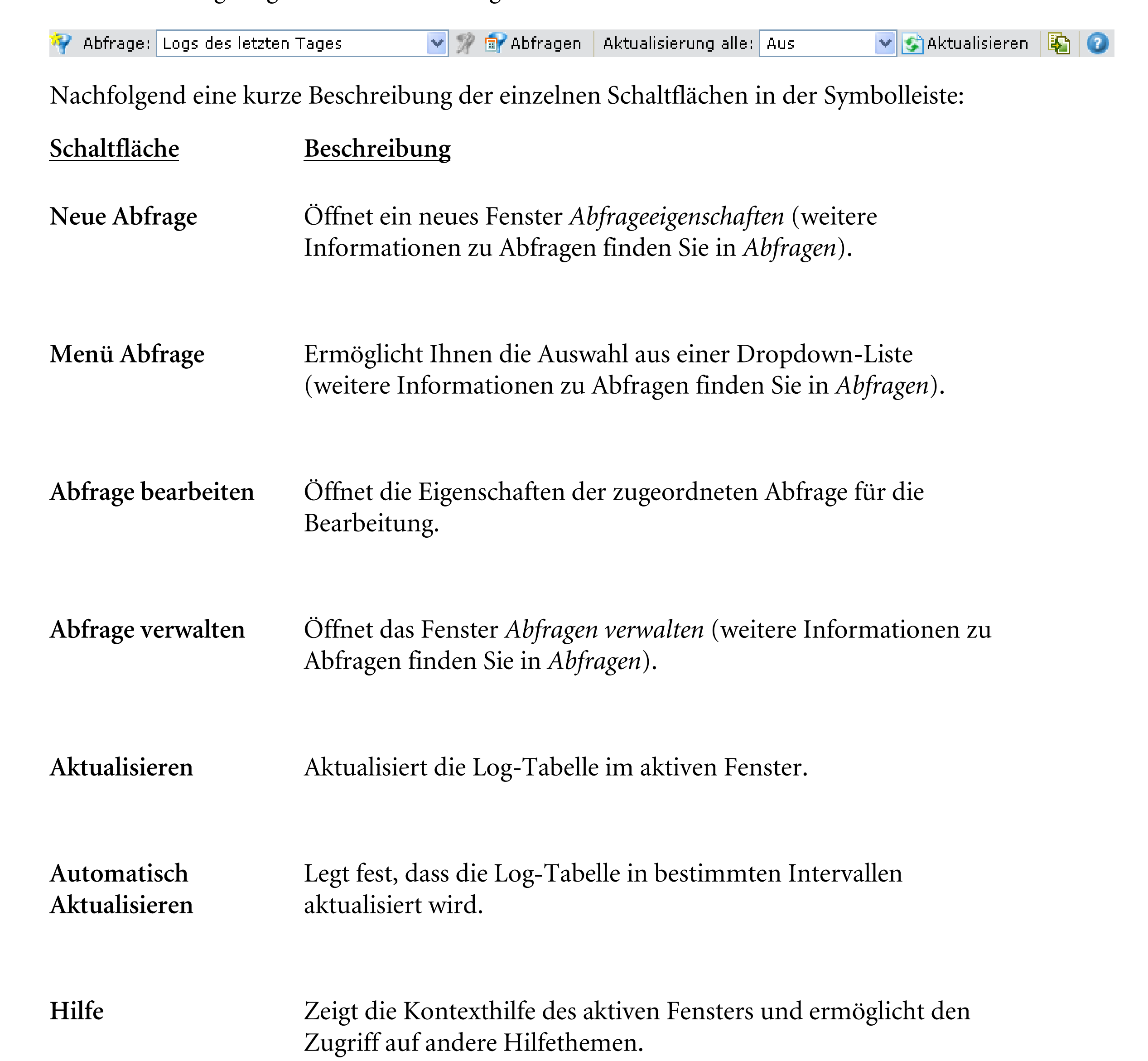
Das Menü *Fenster*, das bei allen Welten gleich ist, ist in *Menü* im Kapitel *Erste Schritte*, beschrieben.

### 5.2.2.6 Menü Hilfe

Das Menü *Hilfe*, das bei allen Welten gleich ist, ist in *Menü* im Kapitel *Erste Schritte*, beschrieben.

## 5.2.3 Symbolleiste

Die Symbolleiste bietet schnellen Zugriff auf häufig genutzte Funktionen. Sie wird unterhalb der Fensterleiste angezeigt und enthält die folgenden Schaltflächen:




Nachfolgend eine kurze Beschreibung der einzelnen Schaltflächen in der Symbolleiste:

| Schaltfläche | Beschreibung |
|---|---|
| **Neue Abfrage** | Öffnet ein neues Fenster *Abfrageeigenschaften* (weitere Informationen zu Abfragen finden Sie in *Abfragen*). |
| **Menü Abfrage** | Ermöglicht Ihnen die Auswahl aus einer Dropdown-Liste (weitere Informationen zu Abfragen finden Sie in *Abfragen*). |
| **Abfrage bearbeiten** | Öffnet die Eigenschaften der zugeordneten Abfrage für die Bearbeitung. |
| **Abfrage verwalten** | Öffnet das Fenster *Abfragen verwalten* (weitere Informationen zu Abfragen finden Sie in *Abfragen*). |
| **Aktualisieren** | Aktualisiert die Log-Tabelle im aktiven Fenster. |
| **Automatisch Aktualisieren** | Legt fest, dass die Log-Tabelle in bestimmten Intervallen aktualisiert wird. |
| **Hilfe** | Zeigt die Kontexthilfe des aktiven Fensters und ermöglicht den Zugriff auf andere Hilfethemen. |

### 5.2.4 Arbeitsbereich

Der Arbeitsbereich ist in zwei Bereiche unterteilt:

- Die **Log-Tabelle** wird im rechten Fensterausschnitt angezeigt und enthält eine Tabelle der Logdatensätze, die von den Client oder vom Management Server empfangen wurden. Wenn sie zum ersten Mal geöffnet wird, enthält sie alle Client-Logs. Die Log-Tabelle ist in *Log-Tabelle beschrieben.*
- Der Bereich im linken Fensterausschnitt enthält die Registerkarten **Organisationsstruktur** und **Nach Namen suchen**. Diese Registerkarten dienen als Filter zur Bestimmung des Ursprungs (d. h. Organisationseinheiten/Computer/Benutzer) der Logdatensätze, die in der Log-Tabelle angezeigt werden. Die Registerkarten werden in *Filtern nach Herkunft des Logdatensatzes* behandelt.
  Diese Registerkarten erscheinen nicht im Fenster Server-Log, weil Server-Logs per Definition nicht für Clients gelten.

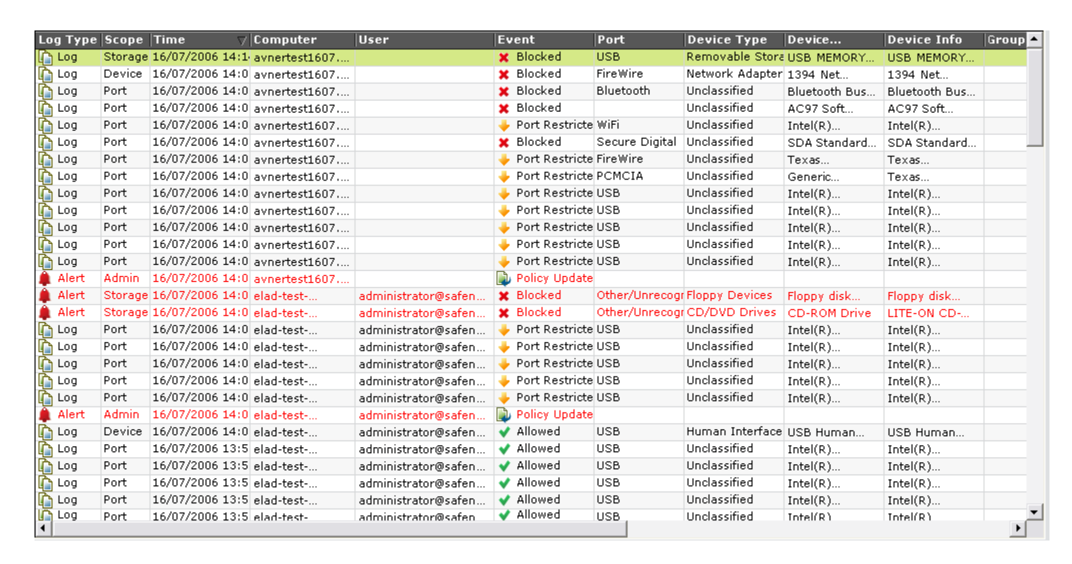
Wenn alle Fenster in der Logs-Welt geschlossen sind, ist der Arbeitsbereich leer. Sie können ein Log-Fenster öffnen, indem Sie auf eine der Startschaltflächen oben rechts im Fenster klicken:
Client Logs | File Logs | Server Logs

Weitere Informationen zum Anzeigen von Logs finden Sie in *Log-Tabelle.*

## 5.3 Log-Tabelle

Die Log-Tabelle (unten in der Abbildung dargestellt) zeigt Informationen zu Ereignissen, die in SafeGuard PortProtector Clients, Management Consoles oder Management Server auftreten. Es gibt drei Argen von Log-Tabellen, die Sie anzeigen und verwalten können:

- **Client-Log –** Dieses Log zeigt Informationen zu Clients und Benutzern in der Organisation. Jeder Datensatz meldet ein bestimmtes Ereignis, wie etwa das Anschließen eines abnehmbaren Geräts an einem Computer, einen Manipulationsversuch etc.
  Eine Beschreibung der Logstruktur finden Sie in *Struktur des Client-Logs.*
- **Datei-Log –** Wenn die Funktion der Dateiprotokollierung für Wechselspeichergeräte, externe Festplattenlaufwerke oder CD/DVDs aktiviert ist, werden die Datei-Informationen in diesem Log angezeigt. Eine Beschreibung der Logstruktur finden Sie in *Struktur des Datei-Logs.* File-Shadowing-Logs werden ebenfalls hier gezeigt.
- **Server-Log –** Dieses Log zeigt Informationen zu Management Server und administrativen Aktionen. Jeder Datensatz meldet ein bestimmtes Ereignis, wie etwa die Anmeldung bei der Management Console, das ändern globaler Policy-Einstellungen etc.



| Log Type | Scope | Time | Computer | User | Event | Port | Device Type | Device... | Device Info | Group |
|---|---|---|---|---|---|---|---|---|---|---|
| Log | Storage | 16/07/2006 14:1 | avnertest1607.... | | Blocked | USB | Removable Stora | USB MEMORY... | USB MEMORY... | |
| Log | Device | 16/07/2006 14:0 | avnertest1607.... | | Blocked | FireWire | Network Adapter | 1394 Net... | 1394 Net... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Blocked | Bluetooth | Unclassified | Bluetooth Bus... | Bluetooth Bus... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Blocked | | Unclassified | AC97 Soft... | AC97 Soft... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Port Restricte | WiFi | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Blocked | Secure Digital | Unclassified | SDA Standard... | SDA Standard... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Port Restricte | FireWire | Unclassified | Texas... | Texas... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Port Restricte | PCMCIA | Unclassified | Generic... | Texas... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 14:0 | avnertest1607.... | | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Alert | Admin | 16/07/2006 14:0 | avnertest1607.... | | Policy Update | | | | | |
| Alert | Storage | 16/07/2006 14:0 | elad-test-... | administrator@safen... | Blocked | Other/Unrecogr | Floppy Devices | Floppy disk... | Floppy disk... | |
| Alert | Storage | 16/07/2006 14:0 | elad-test-... | administrator@safen... | Blocked | Other/Unrecogr | CD/DVD Drives | CD-ROM Drive | LITE-ON CD-... | |
| Log | Port | 16/07/2006 14:0 | elad-test-... | administrator@safen... | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 14:0 | elad-test-... | administrator@safen... | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 14:0 | elad-test-... | administrator@safen... | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 14:0 | elad-test-... | administrator@safen... | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 14:0 | elad-test-... | administrator@safen... | Port Restricte | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Alert | Admin | 16/07/2006 14:0 | elad-test-... | administrator@safen... | Policy Update | | | | | |
| Log | Device | 16/07/2006 14:0 | elad-test-... | administrator@safen... | Allowed | USB | Human Interface | USB Human... | USB Human... | |
| Log | Port | 16/07/2006 13:5 | elad-test-... | administrator@safen... | Allowed | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 13:5 | elad-test-... | administrator@safen... | Allowed | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 13:5 | elad-test-... | administrator@safen... | Allowed | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 13:5 | elad-test-... | administrator@safen... | Allowed | USB | Unclassified | Intel(R)... | Intel(R)... | |
| Log | Port | 16/07/2006 13:5 | elad-test- | administrator@safen | Allowed | USB | Unclassified | Intel(R) | Intel(R) | |

Die obige Abbildung zeigt das Client-Log. File-Logs und Server-Logs zeigen unterschiedliche Informationen.

Standardmäßig wird in der anfänglichen Log-Tabelle das Clients-Log mit allen Datensatztypen für alle Clients und Benutzer in die Organisation angezeigt. Sie können weitere Fenster mit zusätzlichen Logtypen öffnen – Client Logs, Server Logs oder File Logs. Eine detaillierte Erklärung der Tabellenstrukturen finden Sie am Ende dieses Kapitels in *Struktur der Log-Tabellen*.

Sie können die Tabellenansicht folgendermaßen ändern:

- **Sortieren** Sie die Tabelle, indem Sie auf den Spaltentitel der Spalte klicken, nach der Sie sortieren möchten. Klicken Sie nochmals auf die Überschrift, um zwischen auf- und absteigender Reihenfolge zu wechseln. Sie können eine zweite Sortierebene hinzufügen, indem Sie die **Umschalttaste** drücken und auf den zweiten Spaltentitel klicken.
- **Ändern Sie die Spaltenbreite**, indem Sie die Spaltentrennlinien an die gewünschte Stelle ziehen.
- **Verschieben Sie eine Spalte**, indem Sie sie an die gewünschte Position ziehen.
- **Filtern nach Log-Herkunft:** Hiermit können Sie die Logdatensätze auf diejenigen beschränken, die von bestimmten Computern/Benutzern oder Organisationseinheiten strammen. Eine umfassende Erläuterung dieser Optionen finden Sie in *Filtern nach Herkunft des Logdatensatzes*. Dort werden die Registerkarten Organisationsstruktur und Nach Namen suchen besprochen (die nicht für Server-Logs gelten).
- **Abfragen:** Es können Abfragen erstellt werden, um Datensätze anhand verschiedener Parameter zu selektieren, wie etwa Datensatztyp, Zeit, Gerätetyp etc. Eine umfassende Erläuterung der Abfragen finden Sie in *Abfragen*.

### 5.3.1 Anzeigen weiterer Datensätze

Die Log-Tabelle zeigt die ersten 1.000 Datensätze, die Ihren Abfrage-/Filterkriterien entsprechen. Wenn Sie zusätzlich ältere Datensätze anzeigen möchten, können Sie hierfür die Schaltflächen zum Blättern unterhalb der Log-Tabelle benutzen. (⏮ « 1 2 3 4 5 »).

So navigieren Sie zu älteren oder neueren Logdatensätzen:

Verwenden Sie die Schaltflächen zum Blättern unterhalb der Log-Tabelle. Sie können entweder auf eine bestimmte Seitenzahl klicken, oder Sie klicken auf **Nächste Seite** (»), **Vorige Seite** («) oder **Erste Seite** (⏮), um in den Seiten des Logs zu navigieren.

**Hinweis:** Es kann etwas dauern, bis eine neue Seite angezeigt wird, weil neue Daten aus der Datenbank geladen werden müssen.

**Hinweis:** Bei der Anzeige von Seite 2 oder höher der Log-Tabelle ist die automatische Aktualisierung deaktiviert.

### 5.3.2 Aktualisieren der Log-Tabelle

Die Log-Tabelle wird automatisch in vordefinierten, von Ihnen festgelegten Intervallen oder bei einer Ad-hoc-Anforderung aktualisiert. Bei der Aktualisierung werden neue Daten erfasst, die auf dem Management Server angesammelt wurden, und dann in der Log-Tabelle entsprechend der aktuellen Sortiereinstellungen der Tabelle angezeigt.

**So aktualisieren Sie die Log-Tabelle:**

Klicken Sie im Menü *Ansicht* auf **Aktualisieren**, oder klicken Sie auf das Symbol **Aktualisieren** ( ) in der Symbolleiste. Der Log-Tabelle werden neue Logdatensätze hinzugefügt.

**So legen Sie Intervalle für die automatische Aktualisierung fest:**

Wählen Sie das Intervall aus der Dropdown-Liste **Refresh every** in der Symbolleiste.

ODER

1 Wählen Sie im Menü *Ansicht* die Option **Automatisch aktualisieren.** Es wird ein Untermenü angezeigt.

2 Klicken Sie im Untermenü auf das gewünschte Aktualisierungsintervall.

Von diesem Moment an wird die Tabelle im ausgewählten Intervall aktualisiert.

**Hinweis:** Bei der Anzeige ab Seite 2 aufwärts in der Log-Tabelle ist die automatische Aktualisierung deaktiviert.

## 5.3.3 Optionen für Logdatensätze

In der Log-Tabelle stehen für die Logdatensätze mehrere Optionen zur Verfügung. Diese Optionen ermöglichen Ihnen Folgendes:

- Anzeige der Datensatz-Eigenschaften.
- Öffnen der Policy, mit der ein Logdatensatz verknüpft ist.
- Kopieren von USB-Gerätedaten in die Zwischenablage.
- Anzeigen aller Logs für ein/e/en Gerät/Policy/Benutzer/Computer, mit dem/der ein Logdatensatz verknüpft ist.

Diese Optionen werden in den folgenden Abschnitten erläutert.

**So greifen Sie auf die Optionen für Logdatensätze zu:**

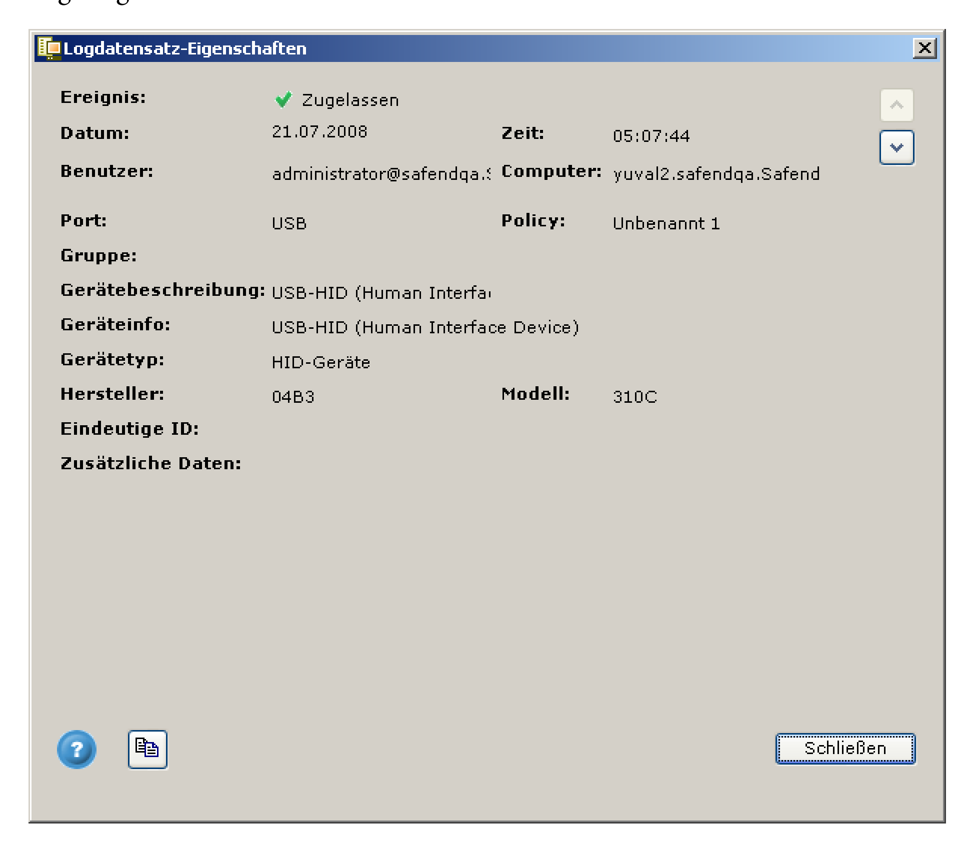
Klicken Sie in der Log-Tabelle mit der rechten Maustaste auf den gewünschten Datensatz. Ein Menü wird angezeigt.

### 5.3.3.1 Anzeigen der Eigenschaften des Logdatensatzes

Diese Option ermöglicht Ihnen die Anzeige der Datensatzeigenschaften in einem Fenster. Sie müssen demnach nicht mehr durch die Log-Tabelle scrollen.

**So zeigen Sie die Datensatzeigenschaften an:**

Klicken Sie im Kontextmenü auf **Eigenschaften**. Das Fenster *Logdatensatz-Eigenschaften* wird angezeigt:



##### 5.3.3.1.1 Logdatensatz-Eigenschaften

Dieses Fenster zeigt die Felder des Datensatzes, abhängig vom Datensatztyp, und die zugehörigen Werte. Für jeden Logtyp (Client, File oder Server) werden andere Information in den entsprechenden Tabellenspalten angezeigt. Eine Erläuterung der Felder finden Sie im Folgenden:

- **Eigenschaften des Client-Logs** – siehe *Struktur des Client-Logs*.
- **Eigenschaften des File-Logs** – siehe *Struktur des Datei-Logs*.
- **Eigenschaften des Server-Logs** – siehe *Struktur des Server-Logs*.

Sie können sich innerhalb des Fensters *Logdatensatz-Eigenschaften* mit Hilfe der Nach-oben- und Nach-unten-Pfeile unten rechts im Fenster zum vorherigen oder nächsten Datensatz bewegen.

Wenn sich der Logdatensatz auf nach ein USB-Gerät oder ein CD/DVD-Medium bezieht, ist die Schaltfläche **Kopieren** unten links im Fenster aktiviert. Über diese Schaltfläche können Sie die Geräte- oder Mediendaten in die Zwischenablage kopieren und dann in eine Gruppe in der weißen Liste einfügen.

**So kopieren Sie USB-Geräte- oder CD/DVD-Mediendaten in die Zwischenablage:**

Klicken Sie auf die Schaltfläche **Kopieren** unten links im Fenster.
Die Geräte-/Medienangaben werden in die Zwischenablage kopiert und können in der Policies-Welt in eine Gruppe in der weißen Liste eingefügt werden.

**So zeigen Sie eine Shadow-Datei an:**

Wählen Sie **Öffnen** oder **Speichern** in der Spalte Shadow-Datei, um die Shadow-Datei aus dem Speicher herunterzuladen.

#### 5.3.3.2 Öffnen der zugeordneten Policy

Über diese Option können Sie die Policy öffnen, die SafeGuard PortProtector Client zum Senden des Logs veranlasst hat, damit Sie ihre Definitionen einsehen können.

**So öffnen Sie die Policy:**

Klicken Sie im Kontextmenü auf **Policy öffnen**. Die Anwendung wechselt in die *Policies*-Welt und zeigt die Policy an, die auf dem Client angewandt ist, der den Logdatensatz gesendet hat.

**Hinweis:** Bei zusammengeführten Policies (siehe *Zusammenführen von Policies*) wird die Policy geöffnet, deren Name in alphabetischer Reihenfolge zuerst kommt.

#### 5.3.3.3 Kopieren von USB-Geräte- oder CD/DVD-Mediendaten

Über diese Option können Sie die Informationen zu dem USB-Gerät oder CD/DVD-Medium, das mit dem Logdatensatz verknüpft ist, in die Zwischenablage kopieren, um sie später beim Freigeben des Geräts/Mediums in einer Policy einzufügen (siehe *Freigeben von Geräten und WiFi-Verbindungen* oder *Freigeben von CD/DVD-Medien* im Kapitel *Definieren von Policies*).

**So kopieren Sie Geräte-/Mediendaten:**

Klicken Sie im Kontextmenü auf **USB-Geräteinformationen kopieren**. Die Geräte-/Medienangaben werden in die Zwischenablage kopiert und können in der Policies-Welt in eine Gruppe in die weiße Liste eingefügt werden(siehe *Hinzufügen von Geräten* und *Hinzufügen von Medien* im Kapitel *Definieren von Policies*).
Dies ist auch über das Fenster *Logdatensatz-Eigenschaften* möglich, wie in *Anzeigen der Eigenschaften des Logdatensatzes* erläutert.

#### 5.3.3.4 Anzeigen aller verknüpften Logdatensätze

Mit dieser Option können Sie alle Logdatensätze anzeigen, die mit demselben Gerät, derselben Policy, demselben Benutzer oder demselben Computer verknüpft sind, zu dem bzw. zu der eine Verknüpfung zum ausgewählten Datensatz besteht.

**So zeigen Sie alle verknüpften Logs an:**

1 Klicken Sie im Kontextmenü auf **Alle Logs anzeigen.** Es wird ein Untermenü angezeigt.

2 Wählen Sie im Untermenü die anzuzeigenden Logdatensätze aus (Von diesem Gerät, Von dieser Policy, Von diesem Benutzer, Von diesem Computer). Die Log-Tabelle zeigt jetzt alle Datensätze für den ausgewählten Typ.

### 5.3.4 Exportieren der Log-Tabelle

Die Log-Tabelle kann im Fenster *Abfrageergebnisse exportieren* exportiert werden.

So öffnen Sie das Fenster *Abfrageergebnisse exportieren*:

Wählen Sie im Menü *Datei* die Option **Exportieren**. Das Fenster *Abfrageergebnisse exportieren* wird angezeigt:



#### 5.3.4.1 Exportieren von Abfrageergebnissen

Verwenden Sie diese Option, um die Log-Tabelle (d. h. die Abfrageergebnisse) zu exportieren, um sie zu drucken oder weitere Analysen durchzuführen. Die Datei wird im XML-Format gespeichert, das ganz einfach mit MS Excel etc. geöffnet werden kann.

**So exportieren Sie die Abfrageergebnisse:**

1 Klicken Sie auf die Schaltfläche **Durchsuchen**, um einen Pfad auszuwählen oder den Pfad für die exportierte Datei einzugeben. Sie können den Standardnamen verwenden oder ihn ändern.

2 Wenn Sie nur die aktuellsten Datensätze der Abfrageergebnisse auswählen möchten, klicken Sie auf die erste Optionsschaltfläche und geben Sie an, wie viele Seiten Sie exportieren möchten.

3 Wenn Sie alle Seiten der Abfrageergebnisse exportieren möchten, aktivieren Sie die Optionsschaltfläche **Alle Seiten**.

Hinweis: Das Exportieren der gesamten Abfrage kann sehr lange dauern.

4 Klicken Sie auf **OK**. Ein Verlaufsfenster wird angezeigt, und der Export beginnt.

### 5.3.5 Anzeigen weiterer Log-Tabellen

Sie können weitere Log-Fenster öffnen und mehrere Log-Fenster gleichzeitig betrachten. Hierfür haben Sie mehrere Möglichkeiten:

**So öffnen Sie ein neues Log-Fenster:**

Klicken Sie in der oberen rechten Start-Registerkarte auf der Registerkarte der Log-Welt (Client Logs | File Logs | Server Logs) auf die gewünschte Start-Schaltfläche

ODER

im Fenster *Abfragen verwalten* (siehe *Verwalten von Abfragen*).

ODER

1 Wählen Sie im Menü *Datei* die Option **Neu**. Ein zweites Menü wird angezeigt.

2 Wählen Sie aus dem zweiten Menü den zu öffnenden Fenstertyp aus (Client-Logs, Server-Logs oder File-Logs).

Das gewünschte Log-Fenster wird angezeigt.

## 5.4 Filtern nach Herkunft des Logdatensatzes

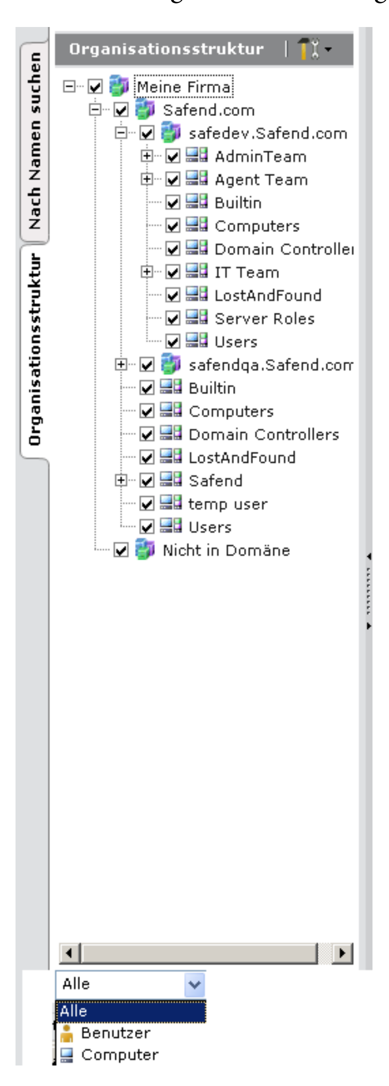
Die linke Seite des Logs-Hauptfensters enthält zwei Registerkarten, die Ihnen helfen die Organisationseinheiten oder Computer/Benutzer zu bestimmen, deren Logs in der Log-Tabelle angezeigt werden sollen. Dabei handelt es sich um die Registerkarten Organisationsstruktur und Suche nach Namen. Dieser Abschnitt gilt nicht für Server-Logs.

### 5.4.1 Filtern der Log-Tabelle nach Organisationseinheit

Die *Organisationsstruktur* ist ein Tool, mit dem Sie die Organisationseinheiten bestimmen können, deren Logdatensätze in Client- oder File-Logs angezeigt werden sollen. Zusammen mit Abfrage (siehe *Abfragen*) wird durch die Auswahl der Elemente in der Organisationsstruktur festgelegt, welche Datensätze in der Log-Tabelle angezeigt werden (siehe *Log-Tabelle*). Dieser Abschnitt beschreibt, wie die Organisationsstruktur gehandhabt und aus der Struktur heraus festgelegt wird, welche Logs und Alarme in der Client- oder Datei-Log-Tabelle angezeigt werden.

Wie bereits erwähnt, erscheint die Struktur nicht im Fenster Server Log, weil Server-Logs per Definition nicht für Computer bzw. Benutzer gelten.

Die Registerkarte *Organisationsstruktur* zeigt die Domäne(n), Organisationseinheiten sowie die Gruppe Nicht in Domäne (die alle Computer enthält, die derzeit zu keiner Domäne gehören), wie in der folgenden Abbildung dargestellt:



**Hinweis:** Die Organisationsstruktur ist nur anwendbar, wenn Sie Active Directory oder Novell eDirectory einsetzen. Andernfalls wird nur eine Gruppe in der Struktur angezeigt – Nicht in Domäne. Durch Auswahl dieser Gruppe werden alle Computer ausgewählt.

**So wählen Sie die gewünschten Organisationseinheiten aus:**

1 Erweitern Sie die Organisationsstruktur ggf., so dass Organisationseinheiten auf niedrigeren Ebenen angezeigt werden.

2 Wählen Sie die gewünschte Domäne oder Organisationseinheiten durch Aktivieren der entsprechenden Kontrollkästchen aus.

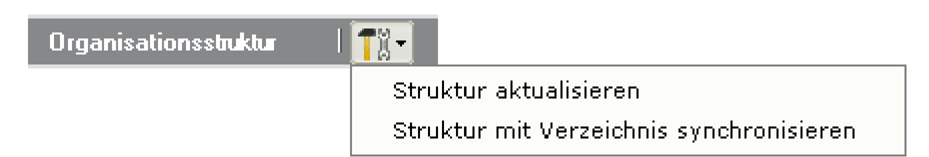
3 Wählen Sie unten in der Registerkarte *Organisationsstruktur* den Typ der anzuzeigenden Objekte aus der Dropdown-Liste aus.




4 Klicken Sie unten auf der Registerkarte *Organisationsstruktur* auf **LOS** . Die Logs, die jetzt in der Log-Tabelle angezeigt werden, stammen ausschließlich von Clients, die zu dem in der Struktur gewählten Element gehören.

#### 5.4.1.1 Aktualisieren der Organisationsstruktur

Bevor Sie Ihre Auswahl in der Struktur treffen, möchten Sie sie vielleicht aktualisieren. Sie können die Struktur entweder im SafeGuard PortProtector Management Server aktualisieren oder sie mit Active Directory/Novell eDirectory synchronisieren (das Directory kann aktueller sein, aber es kann auch länger dauern). Die Struktur wird über das Menü *Organisationsstruktur* (unten dargestellt) aktualisiert, das sich oben in der der Registerkarte Organisationsstruktur befindet.




**So aktualisieren Sie die Organisationsstruktur im Management Server:**

Klicken Sie im Menü *Organisationsstruktur* auf **Struktur aktualisieren.** Die Struktur wird aktualisiert.

**So aktualisieren Sie die Organisationsstruktur im Directory:**

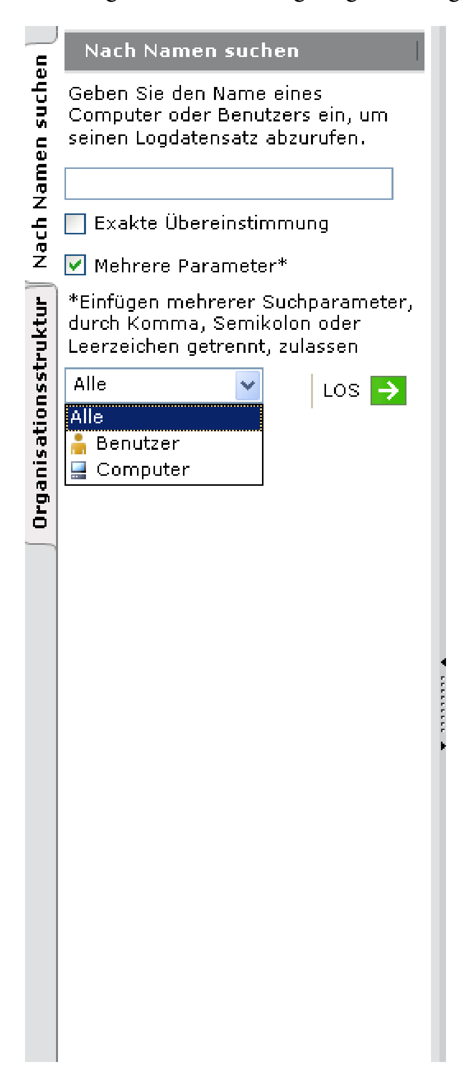
Klicken Sie im Menü *Organisationsstruktur* (siehe vorherige Abbildung) auf **Struktur mit Verzeichnis synchronisieren.** Die Struktur wird aktualisiert, aber dieser Vorgang kann eine Weile dauern.

### 5.4.2 Filtern nach Namen

Die Registerkarte *Nach Namen suchen* ist ein weiteres Werkzeug, mit dem Sie die Computer oder Benutzer bestimmen können, deren Logdatensätze im Client- oder File-Log angezeigt werden. Die von Ihnen hier angegebenen Suchkriterien legen gemeinsam mit Abfragen (siehe *Abfragen*) fest, welche Datensätze in der Log-Tabelle (siehe *Log-Tabelle*) angezeigt werden. Dieser Abschnitt beschreibt, wie diese Registerkarte zur Festlegung der in der Client- oder Datei-Log-Tabelle anzuzeigenden Logs verwendet wird.

Wie bereits erwähnt, erscheint diese Registerkarte nicht im Fenster Server Log, weil Server-Logs per Definition nicht für Computer bzw. Benutzer gelten.

Die folgende Abbildung zeigt die Registerkarte *Nach Namen suchen*:

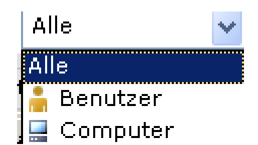


**So suchen Sie nach bestimmten Computern oder Benutzern:**

1 Geben Sie im Textfeld den Namen des Computers oder Benutzers ein, dessen Logdatensätze Sie in der Log-Tabelle anzeigen möchten. Sie können mehrere Namen durch Komma, Semikolon oder Leerzeichen getrennt eingeben.

2 Markieren Sie das Kontrollkästchen **Exakte Übereinstimmung**, wenn Sie in der Log-Tabelle Logs für einen Computer/Benutzer mit einem Namen anzeigen möchten, der genau mit der von Ihnen im Textfeld eingegebenen Zeichenfolge übereinstimmt. Für Computer müssen Sie den vollständigen Computernamen eingeben (einschließlich der Domänenendung). Wenn **Exakte Übereinstimmung** nicht markiert ist, werden in der Log-Tabelle Logs für alle Computer und Benutzer angezeigt, deren Name die von Ihnen eingegebene Zeichenfolge enthält.

3 Wählen Sie im Menü *Nach Namen suchen* die




Option **Computer**, wenn Sie nach Computernamen suchen möchten, bzw. die Option **Benutzer**, wenn Sie nach Benutzernamen suchen möchten, oder die Option **Alle**, wenn Sie nach Computern und Benutzern suchen möchten.

4 Klicken Sie unter dem Textfeld auf **LOS** . Die Logs, die jetzt in der Log-Tabelle angezeigt werden, stammen von dem Computer/Benutzer (einer oder mehrere), dessen Name Ihren Suchkriterien entspricht. Wenn kein Computer oder Benutzer gefunden wird, dessen Name Ihren Suchkriterien entspricht, ist die Log-Tabelle leer.

## 5.5 Abfragen

Ein weiteres Verfahren zur Filterung von Logdatensätzen in der Log-Tabelle ist die Verwendung von Abfragen. Sie können Abfragen nach verschiedenen Kriterien, oder *Eigenschaften* definieren, so dass nur Logdatensätze in der Log-Tabelle erscheinen, die den von Ihnen angegebenen Kriterien entsprechen. Bei Client-Logs und File-Logs interagieren Abfragen mit Ihrer Auswahl in der Organisationsstruktur, um die anzuzeigenden Datensätze zu bestimmen.

Es stehen drei Abfragetypen zur Verfügung, die die drei verfügbaren Logtypen abdecken: Client-Logs-Abfragen, File-Logs-Abfragen und Server-Logs-Abfragen.

Abfragen können ad-hoc definiert und bearbeitet oder für zukünftige Verwendung gespeichert werden. Die Standardabfrage ist Alle Logs, bei der alle Logdatensätze angezeigt werden (um genau zu sein: die Datensätze, die den Auswahlkriterien in der Organisationsstruktur entsprechen).

Nachdem Sie eine Abfrage definiert und gespeichert haben, können Sie sie aus dem Menü **Abfrage** in der Symbolleiste auswählen.

### 5.5.1 Integrierte Abfragen

SafeGuard PortProtector wird mit mehreren integrierten Abfragen geliefert, die Sie bei Bedarf als Ausgangsbasis benutzen können. Dazu gehören die folgenden Client-Logs-und File-Logs-Abfragen (für Server-Logs sind keine integrierten Abfragen vorhanden):

Integrierte Client-Logs-Abfragen

- (**Integriert**) **Alle Alarme:** zeigt alle Client-Alarme, ohne Dateialarme.
- (**Integriert**) **Gesperrte Geräte:** zeigt alle Logs bezüglich der Sperrung von Nicht-Speichergeräten.
- (**Integriert**) **Gesperrte Speichergeräte:** zeigt alle Logs bezüglich der Sperrung von Speichergeräten.
- (**Integriert**) **Interne Port-Ereignisse:** zeigt alle Logs bezüglich interner Logereignisse.
- (**Integriert**) **Suspendierungs-Ereignisse:** zeigt alle Administrationsereignisse bezüglich Client-Suspendierungen.
- (**Integriert**) **Manipulations-Ereignisse:** zeigt alle Manipulationsversuche.
- (**Integriert**) **WiFi-Ereignisse:** zeigt alle Logs bezüglich WiFi-Ereignissen.

Integrierte File-Logs-Abfragen

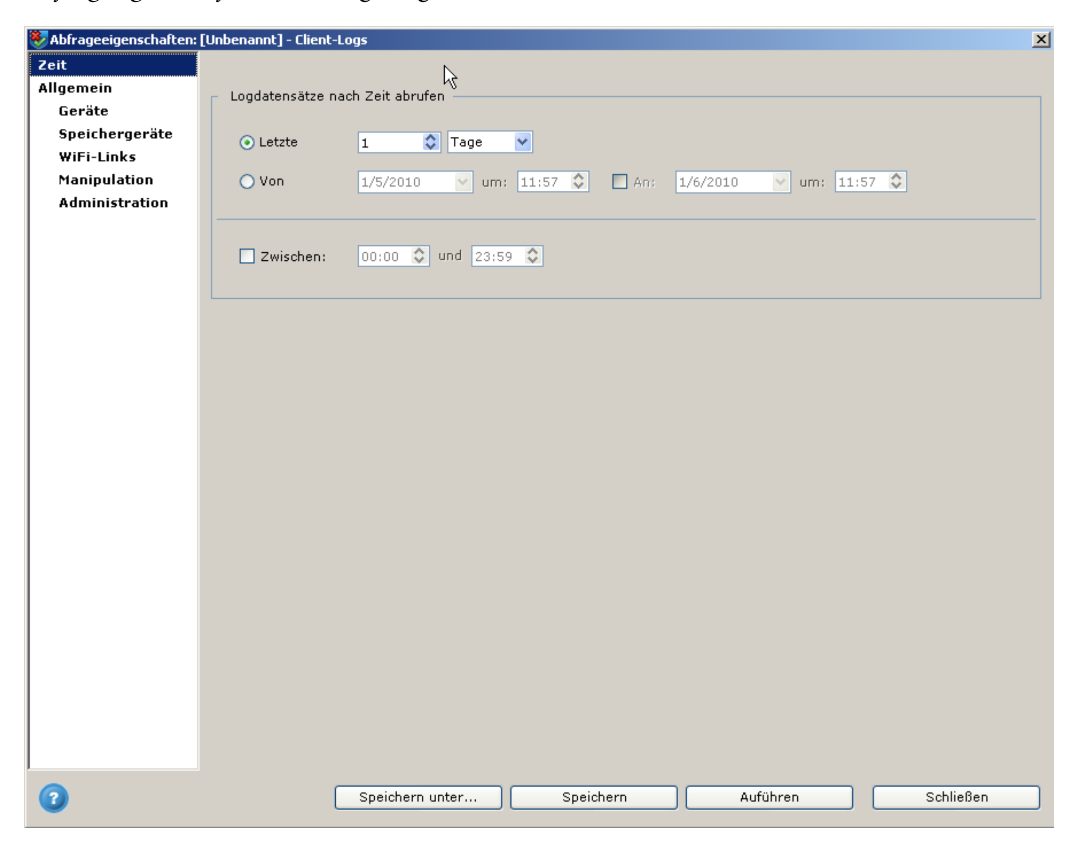
- (**Integriert**) **Alle Dateialarme:** zeigt alle Dateialarme.
- (**Integriert**) **Gesperrte Lesedateien:** zeigt alle Logs bezüglich der gesperrter Dateien, die von Speichergeräten gelesen werden.
- (**Integriert**) **Gesperrte geschriebene Dateien:** zeigt alle Logs bezüglich der gesperrter Dateien, die auf Speichergeräte geschrieben werden.
- (**Integriert**) **Offline-Ereignisse:** zeigt alle Logs bezüglich Ereignissen, die auftraten, als ein verschlüsseltes Wechselspeichergerät von einem autorisierten Endbenutzer auf einem firmenfremden Computer benutzt wurde.
- (**Integriert**) **Sensible Inhaltsprüfungsergebnisse:** zeigt alle Dateiereignisse bezüglich sensibler Inhalte (nutzen Sie diese Abfrage nur, wenn Sie die Inhaltsprüfung aktiviert haben).

## 5.5.2 Definieren einer neuen Client-Log-Abfrage

Abfragen werden im Fenster *Abfrageeigenschaften* definiert. Für jeden Logtyp (Client-, Server- oder File-Logs) steht ein anderes Fenster zur Verfügung. Dieser Abschnitt befasst sich mit Client-Logs-Abfragen. Informationen zum Definieren von File-Log-Abfragen finden Sie in *Definieren einer neuen Datei-Log-Abfrage*. Informationen zum Definieren von Server-Log-Abfragen finden Sie in *Definieren einer neuen Server-Log-Abfrage*.

**So öffnen Sie das Fenster Abfrageeigenschaften:**

Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Abfrage**. Das Fenster *Abfrageeigenschaften* wird angezeigt:




Alternativ hierzu können Sie dieses Fenster aus dem Fenster *Abfragen verwalten* heraus öffnen (siehe *Verwalten von Abfragen*).

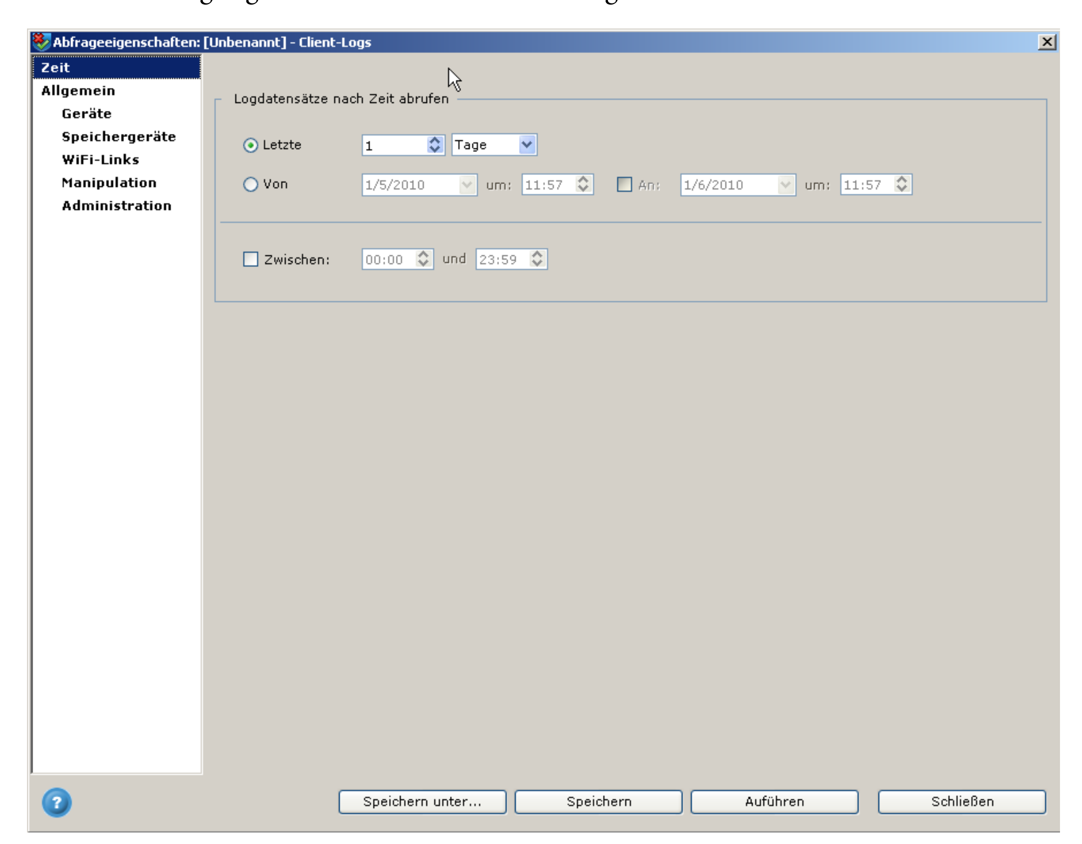
Das Fenster *Abfrage* (siehe vorherige Abbildung) ist in zwei Bereiche unterteilt:

- **Im linken Abschnitt** stehen die Namen der verschiedenen Registerkarten, in denen Sie die Abfrageeigenschaften definieren können. Es gibt zwei Hauptregisterkarten, *Zeit* und *Allgemein*. Abhängig vom Logtyp stehen zusätzliche Registerkarten zur Verfügung, die detaillierte Definitionen zu den Themen im Fenster *Allgemein* enthalten.
- **Der rechte Abschnitt** zeigt die Registerkarte *Abfrageeigenschaften*, die die entsprechenden Definitionen für die Auswahl im linken Abschnitt enthält. Die auf dieser Registerkarte gemachten Definitionen bilden die Kriterien dafür, welche Datensätze in der Log-Tabelle angezeigt werden. Die Datensätze müssen den definierten Kriterien entsprechen.

Hier werden jetzt die verschiedenen Definitionen und deren Funktionsweise besprochen.

### 5.5.2.1 Zeiteigenschaften – Client-Logs

Die Zeit-Abfrageeigenschaften werden auf der Registerkarte *Zeit* definiert:




#### 5.5.2.1.1 Definieren von Zeiteigenschaften – Client-Logs

Auf der Registerkarte *Zeit* definieren Sie den Zeitrahmen für die anzuzeigenden Datensätze. Unabhängig von anderen Abfragedefinitionen werden die Datensätze in der Log-Tabelle den von Ihnen hier festgelegten Zeitkriterien entsprechen.

**So definieren Sie Zeiteigenschaften:**

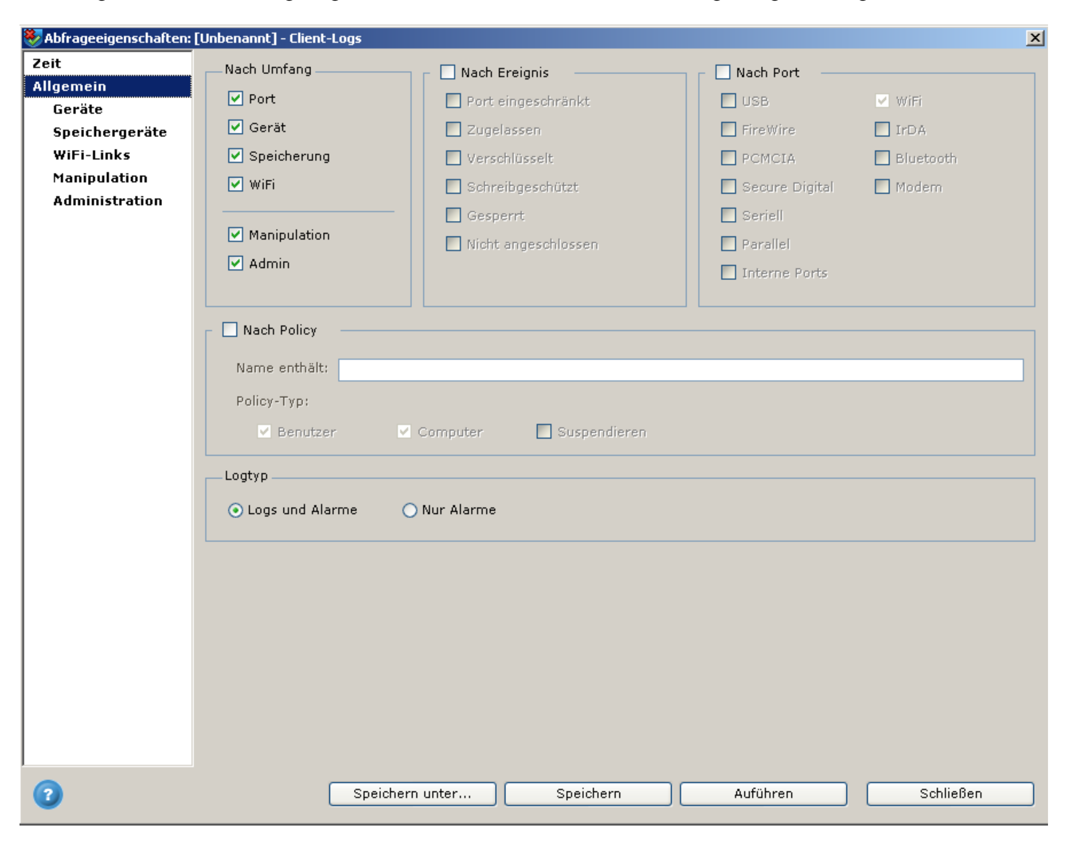
Geben Sie auf der Registerkarte *Zeit* den gewünschten Zeitrahmen für Logdatensätze ein. Die folgenden Optionen sind verfügbar:

- Klicken Sie auf die Optionsschaltfläche **Letzte**, um einen Zeitraum relativ zum aktuellen Tag auszuwählen. Wenn Sie möchten, geben Sie ein Zeitfenster für die Tage im ausgewählten Zeitraum an, indem Sie das Kontrollkästchen **Zwischen** markieren.
- Klicken Sie auf die Optionsschaltfläche **Von**, um ein definitives Datum und eine definitive Zeit auszuwählen, ab wann Datensätze angezeigt werden sollen. Markieren Sie das Kontrollkästchen **Bis**, wenn Sie ein definitives Enddatum und eine definitive Endzeit festlegen möchten, so dass nur Datensätze angezeigt werden, die zwischen die **Von**- und **Bis**-Zeit fallen.

Als Ergebnis werden nur Datensätze in der Log-Tabelle angezeigt, die Ihrer Auswahl entsprechen.

### 5.5.2.2 Allgemeine Abfrageeigenschaften – Client-Logs

Die allgemeinen Abfrageeigenschaften werden auf der hier gezeigten Registerkarte definiert:




#### 5.5.2.2.1 Definieren von allgemeinen Abfrageeigenschaften – Client-Logs

Auf der Registerkarte *Allgemein* definieren Sie, welche Logdatensätze in der Log-Tabelle angezeigt werden, indem Sie Umfang, Port, Ereignis und andere Eigenschaften angeben. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen.

Im Folgenden werden die Abschnitte dieser Registerkarte beschrieben:

- **Nach Umfang** – In diesem Abschnitt können Sie den Umfang festlegen, der in die Log-Tabelle aufgenommen werden soll (Sie können mehrere Typen auswählen). Wenn Sie keinen auswählen, werden die Datensätze unabhängig von dem Umfang, für den sie gelten, angezeigt.

**Hinweis:** Sie können bestimmte Eigenschaften für jede Umfangsart definieren. Die Porteigenschaften werden im Abschnitt Port auf der Registerkarte *General* definiert. Die Eigenschaften bezüglich der anderen Umfangsarten werden auf den anderen Registerkarten, die entsprechend benannt sind, definiert (Geräteeigenschaften werden auf der Registerkarte Geräte, Speichergeräteeigenschaften auf der Registerkarte Speichergeräte etc. definiert).

- **Nach Ereignis** – In diesem Abschnitt können Sie das Ereignis festlegen, das in die Log-Tabelle aufgenommen werden soll (Sie können mehrere Ereignisse auswählen). Wenn Sie keins auswählen, werden die Datensätze unabhängig von dem Ereignis, für das sie gelten, angezeigt.

**Hinweis:** In diesem Abschnitt sind nur Ereignistypen verfügbar, die für Ihre Auswahl unter Nach Umfang relevant sind. Das bedeutet: Wenn Sie alle Umfangsarten gewählt haben, sind alle Optionen für Nach Ereignis aktiviert. Wenn Sie jedoch beispielsweise nur die Umfangsart Port wählen, sind nur die Ereignisoptionen Port eingeschränkt und Gesperrt aktiviert.

**Hinweis:** Wenn Sie nur Manipulation bzw. **Administration** unter Nach Umfang auswählen, ist der Abschnitt Nach Ereignis deaktiviert, da er für diese Umfangsarten nicht relevant ist.

- **Nach Port** – In diesem Abschnitt können Sie den Port festlegen, der in die Log-Tabelle aufgenommen werden soll (Sie können mehrere Ports auswählen). Wenn Sie diesen Abschnitt nicht auswählen, werden die Datensätze unabhängig von dem Port, für den sie gelten, angezeigt.

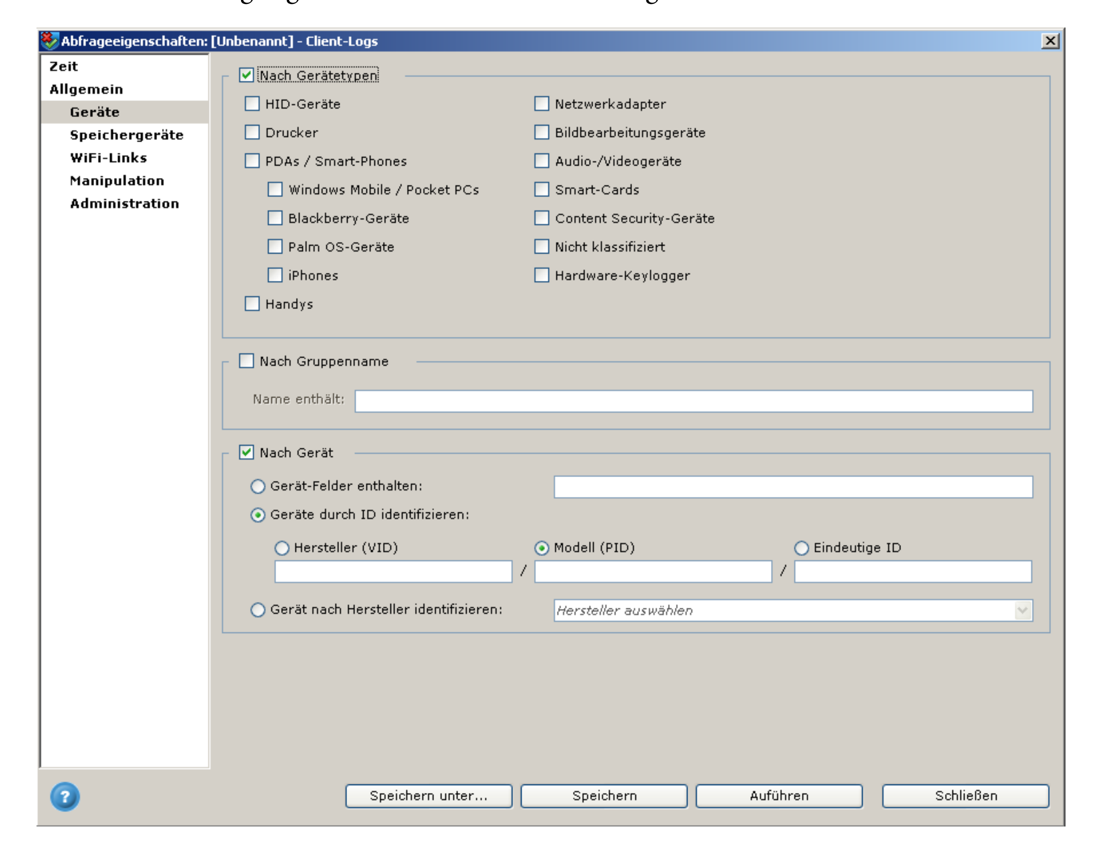
**Hinweis:** In diesem Abschnitt sind nur Ports verfügbar, die für Ihre Auswahl unter Nach Umfang relevant sind. Das bedeutet: Wenn Sie alle Umfangsarten gewählt haben, sind alle Optionen für By Port aktiviert. Wenn Sie jedoch beispielsweise nur die Umfangsart Storage wählen, sind nur die Portoptionen USB, FireWire und PCMCIA aktiviert.

**Hinweis:** Wenn Sie nur Manipulation bzw. Admin unter Nach Umfang auswählen, ist der Abschnitt Nach Port deaktiviert, da er für diese Umfangsarten nicht relevant ist.

- **Nach Policy** – In diesem Abschnitt können Sie den Namen (ganz oder teilweise) der Policy bzw. Policies eingeben, die mit den Datensätzen in der Log-Tabelle verknüpft werden sollen. Es werden nur Policies angezeigt, deren Name den von Ihnen eingegebenen Text enthält. Wenn Sie diesen Abschnitt auswählen, werden in der Log-Tabelle Datensätze unabhängig von der Policy, mit der sie verknüpft sind, angezeigt.
  Wenn Sie diesen Abschnitt auswählen, müssen Sie einen der Policy-Typen auswählen.
- **Logtyp** – In diesem Abschnitt können Sie wählen, ob Sie Log- and Alarmdatensätze oder nur Alarme anzeigen möchten.

### 5.5.2.3 Geräteeigenschaften – Client-Logs

Die Geräte-Abfrageeigenschaften werden auf der Registerkarte *Geräte* definiert:



#### 5.5.2.3.1 Definieren von Geräte-Abfrageeigenschaften – Client-Logs

Auf der Registerkarte **Geräte** definieren Sie die anzuzeigenden Logdatensätze bezüglich ihrer Geräteattribute. Es werden nur Datensätze angezeigt, die den von Ihnen hier festgelegten Kriterien entsprechen.

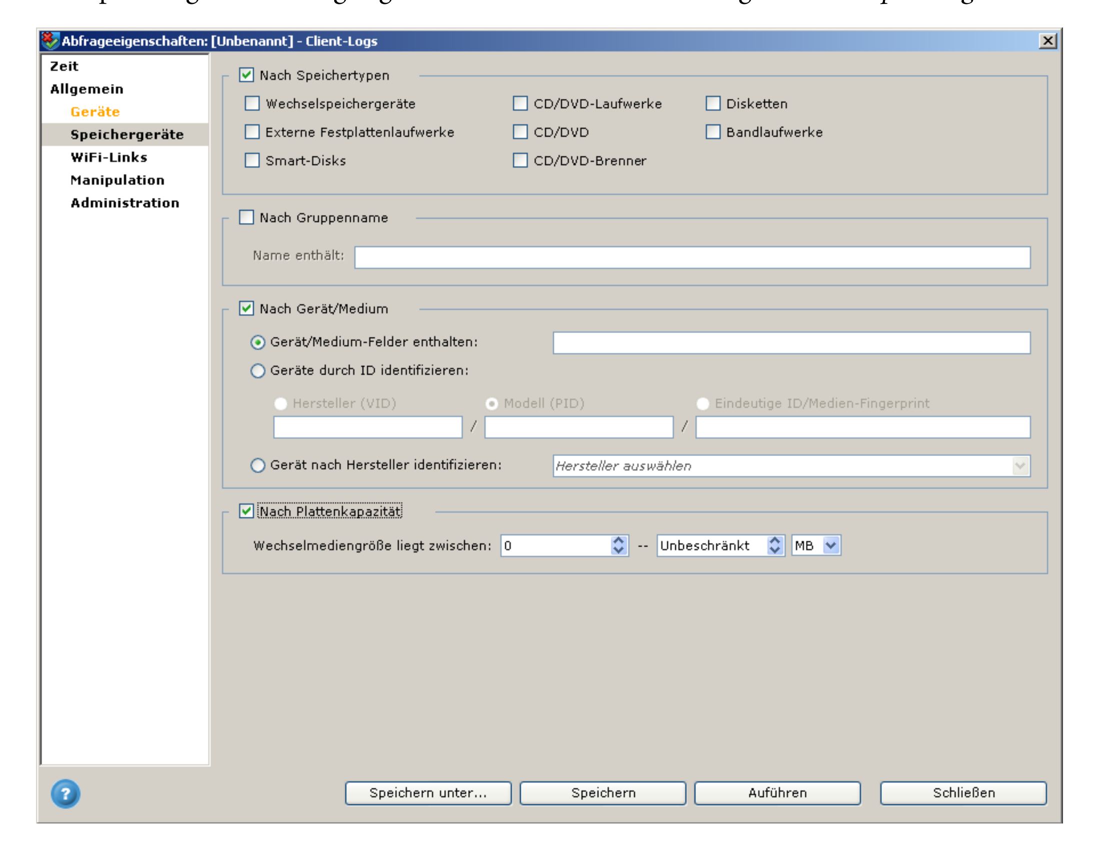
**Hinweis:** Diese Registerkarte ist nur dann aktiviert, wenn Sie **Gerät** im Abschnitt *Umfang* der Registerkarte *Allgemein* auswählen.

Im Folgenden werden die Abschnitte dieser Registerkarte beschrieben:

- **Nach Gerätetypen –** In diesem Abschnitt können Sie den Gerätetyp festlegen, der in die Log-Tabelle aufgenommen werden soll (Sie können mehrere Typen auswählen). Wenn Sie diesen Abschnitt nicht auswählen, werden die Datensätze unabhängig von dem Gerätetyp, für den sie gelten, angezeigt.
- **Nach Gruppenname –** In diesem Abschnitt können Sie den Namen (ganz oder teilweise) der Gerätegruppe eingeben, die in die Log-Tabelle aufgenommen werden soll. Es werden nur Geräte angezeigt, die zu diesen Gruppen gehören. Wenn Sie keinen Gruppennamen eingeben, werden in der Log-Tabelle Datensätze unabhängig von der Gruppe angezeigt, der sie angehören.
- **Nach Gerät –** In diesem Abschnitt können Sie die Geräte auswählen, die in die Log-Tabelle aufgenommen werden sollen. Sie können sie durch Eingabe des Gerätenamens (ganz oder teilweise) oder der Vendor-ID, des Modells oder der Distinct-ID auswählen. Wenn Sie in diesem Abschnitt keine Auswahl treffen, werden Datensätze für alle Geräte angezeigt.

### 5.5.2.4 Speichergeräteeigenschaften – Client-Logs

Die Speichergeräte-Abfrageeigenschaften werden auf der Registerkarte *Speichergeräte* definiert:



##### 5.5.2.4.1 Definieren von Speichergeräteeigenschaften – Client-Logs

Auf der Registerkarte **Speichergeräte** definieren Sie die anzuzeigenden Logdatensätze bezüglich ihrer Speichergeräteattribute. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen.

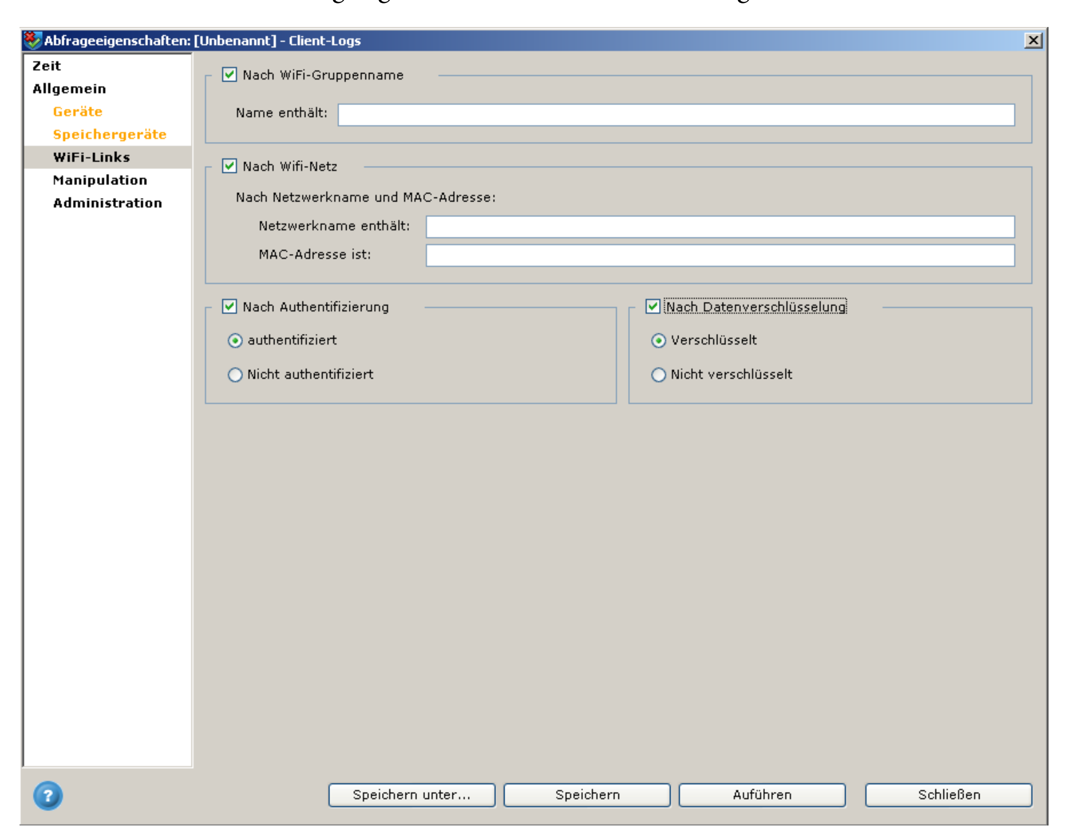
Hinweis: Diese Registerkarte ist nur dann aktiviert, wenn Sie **Speicher** im Abschnitt **Umfang** der Registerkarte *Allgemein* auswählen oder keine Auswahl treffen (was der Auswahl von 'Alle' entspricht).

Im Folgenden werden die Abschnitte dieser Registerkarte beschrieben:

- **Nach Speichertypen –** In diesem Abschnitt können Sie den Speichergerätetyp festlegen, der in die Log-Tabelle aufgenommen werden soll (Sie können mehrere Typen auswählen). Wenn Sie diesen Abschnitt nicht auswählen, werden die Datensätze unabhängig von dem Speichergerätetyp, für den sie gelten, angezeigt.
- **Nach Gruppenname –** In diesem Abschnitt können Sie den Namen (ganz oder teilweise) der Speichergerätegruppe eingeben, die in die Log-Tabelle aufgenommen werden soll. Es werden nur Geräte angezeigt, die zu diesen Gruppen gehören. Wenn Sie keinen Gruppenname eingeben, werden in der Log-Tabelle Datensätze unabhängig von der Gruppe angezeigt, der sie angehören.
- **Nach Gerät/Medium –** In diesem Abschnitt können Sie die Speichergeräte auswählen, die in die Log-Tabelle aufgenommen werden sollen. Sie können sie auswählen, indem Sie Text aus dem Geräte- oder CD/DVD-Mediennamen oder einem anderen Textfeld (ganz oder teilweise) oder Vendor-ID, Modell oder Distinct-ID, oder – bei CD/DVD – ihren Fingerprint eingeben. Wenn Sie in diesem Abschnitt keine Auswahl treffen, werden Datensätze für alle Geräte, die zu den Speichergerätetypen gehören, angezeigt.
- **Nach Plattenkapazität –** Wenn Sie Nach Speichertypen (siehe oben), **Wechselspeichergeräte** oder **Externe Festplattenlaufwerke** wählen, können Sie in diesem Abschnitt den Bereich der Mediengröße definieren, der in die Log-Tabelle aufgenommen werden soll. Wenn Sie keine auswählen, werden in der Log-Tabelle Datensätze für Speichergeräte unabhängig von ihrer Kapazitätsgröße angezeigt.

### 5.5.2.5 WiFi-Verbindungseigenschaften – Client-Logs

Die WiFi-Anschluss-Abfrageeigenschaften werden auf der Registerkarte *WiFi Links* definiert:




#### 5.5.2.5.1 Definieren von WiFi-Verbindungseigenschaften – Client-Logs

Auf der Registerkarte **WiFi-Links** definieren Sie die anzuzeigenden Logdatensätze bezüglich ihrer WiFi-Attribute. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen.

**Hinweis:** Diese Registerkarte ist nur dann aktiviert, wenn Sie **WiFi** im Abschnitt *Umfang* der Registerkarte *Allgemein* auswählen.

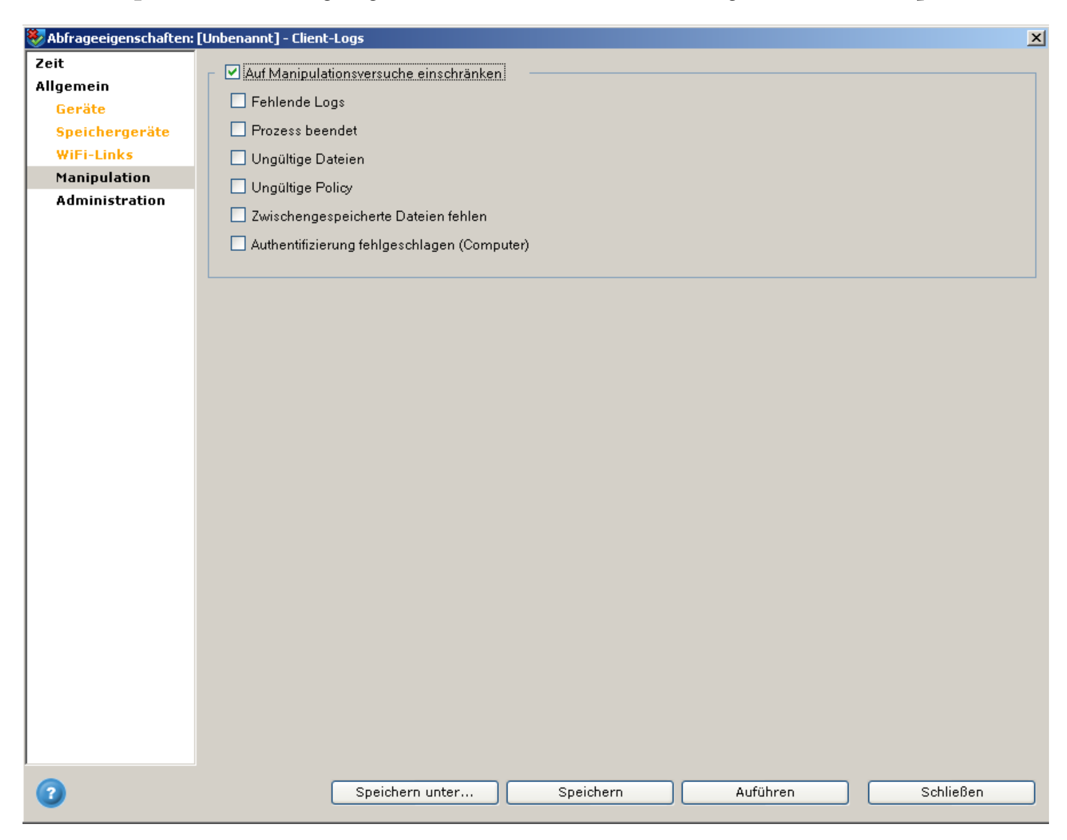
Im Folgenden werden die Abschnitte dieser Registerkarte beschrieben:

- **Nach WiFi-Gruppenname –** In diesem Abschnitt können Sie den Namen (ganz oder teilweise) der WiFi-Gruppe eingeben, die in die Log-Tabelle aufgenommen werden soll. Es werden nur Logdatensätze angezeigt, die mit den zu dieser Gruppe gehörenden WiFi-Verbindungen verknüpft sind. Wenn Sie keinen Gruppennamen eingeben, werden in der Log-Tabelle Datensätze unabhängig von der Gruppe angezeigt, der sie angehören.
- **Nach WiFi-Netz –** In diesem Abschnitt können Sie den Namen (ganz oder teilweise) das Netzwerk bzw. dessen MAC-Adresse eingeben, das in die Log-Tabelle aufgenommen werden soll. Es werden nur Logdatensätze mit den ausgewählten Netzeigenschaften angezeigt. Wenn Sie keine Netzwerkeigenschaften eingeben, werden in der Log-Tabelle Datensätze unabhängig von dem Netz, mit dem sie verknüpft sind, angezeigt.

- **Nach Authentifizierung –** In diesem Abschnitt können Sie festlegen, ob die WiFi-Links in der Log-Tabelle authentifizierte Verbindungen sein sollen. Ansonsten, wenn Sie z. B. Logdatensätze für authentifizierte und nicht authentifizierte Verbindungen wünschen, wählen Sie diesen Abschnitt nicht aus.
- **Nach Datenverschlüsselung –** In diesem Abschnitt können Sie festlegen, ob die WiFi-Verbindungen in der Log-Tabelle verschlüsselte Verbindungen sein sollen.

### 5.5.2.6 Manipulationseigenschaften – Client-Logs

Die Manipulations-Abfrageeigenschaften werden auf der Registerkarte *Manipulation* definiert:




#### 5.5.2.6.1 Definieren von Manipulationseigenschaften – Client-Logs

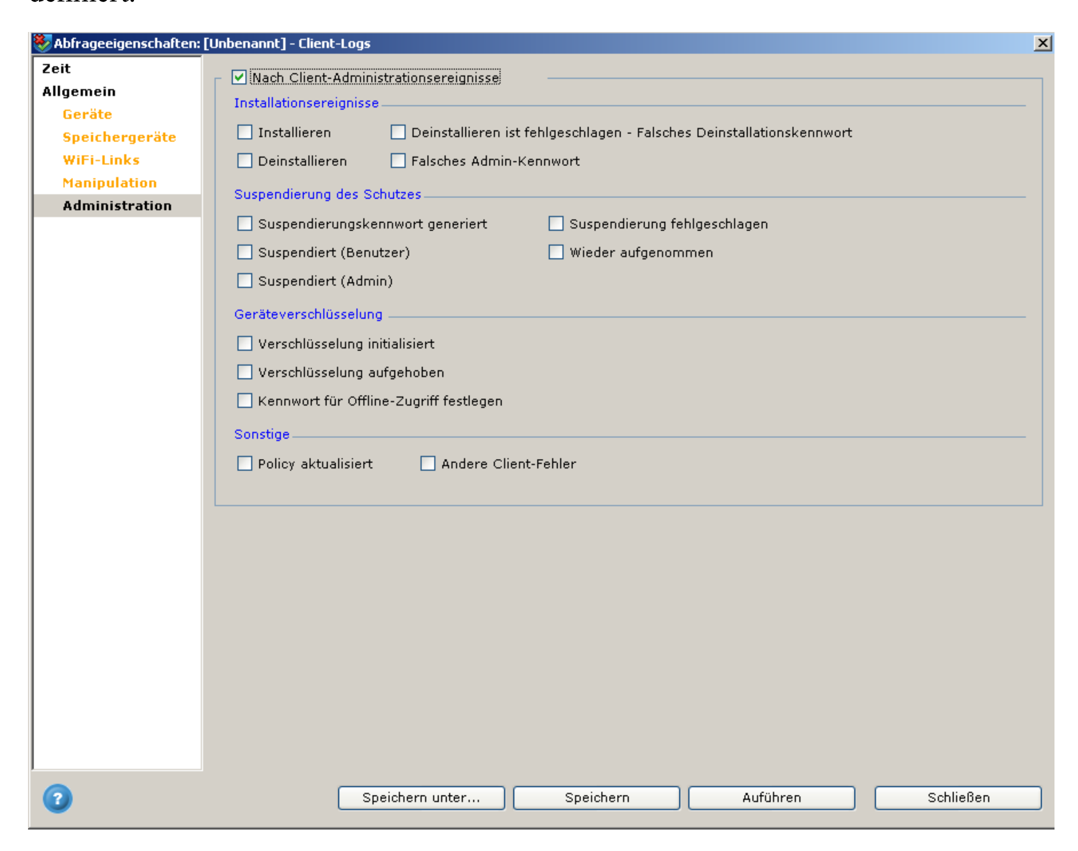
Auf der Registerkarte *Manipulation* definieren Sie die anzuzeigenden Logdatensätze bezüglich der Ereignisse ihrer Manipulationsversuche. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen.

**Hinweis:** Diese Registerkarte ist nur dann aktiviert, wenn Sie **Manipulation** im Abschnitt *Umfang* der Registerkarte *Allgemein* auswählen.

Im Abschnitt Auf Manipulationsversuche einschränken können Sie die Art des Versuchs festlegen, der in die Log-Tabelle aufgenommen werden soll (Sie können mehrere Ereignisse auswählen). Wenn Sie diesen Abschnitt nicht auswählen, werden die Datensätze unabhängig von dem Manipulationsversuch, für den sie gelten, angezeigt.

### 5.5.2.7 Administrationseigenschaften – Client-Logs

Die Administrations-Abfrageeigenschaften werden auf der Registerkarte *Administration* definiert:




#### 5.5.2.7.1 Definieren von Administrationseigenschaften – Client-Logs

Auf der Registerkarte *Administration* definieren Sie die anzuzeigenden Logdatensätze bezüglich ihrer Administrationsereignisse. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen.

**Hinweis:** Diese Registerkarte ist nur dann aktiviert, wenn Sie **Administration** im Abschnitt *Umfang* der Registerkarte *Allgemein* auswählen.

**Nach Client-Administrationsereignissen** – Markieren Sie dieses Kontrollkästchen, um die Client-Administrationsereignisse auszuwählen, die in die Log-Tabelle aufgenommen werden sollen. Die Ereignisse sind in Gruppen angeordnet. Sie können Ereignisse aus verschiedenen Gruppen auswählen, und in jeder Gruppe können Sie mehr als ein Ereignis auswählen.

Wenn Sie diesen Abschnitt nicht auswählen, werden die Datensätze unabhängig von dem Client-Administrationsereignis, für das sie gelten, angezeigt.

Im Folgenden werden die Gruppen auf dieser Registerkarte beschrieben:

- **Installationsereignisse** – In dieser Gruppe können Sie die Installationsereignisse auswählen, die in die Log-Tabelle aufgenommen werden sollen.
- **Suspendierung des Schutzes** – In dieser Gruppe können Sie die Schutzsaufhebungsereignisse auswählen, die in die Log-Tabelle aufgenommen werden sollen.

- **Geräteverschlüsselung** – In dieser Gruppe können Sie die Geräteverschlüsselungsereignisse auswählen, die in die Log-Tabelle aufgenommen werden sollen.
- **Sonstige** – Klicken Sie in dieser Gruppe auf die Kontrollkästchen, um die Datensätze anzuzeigen, die für Policy-Aktualisierung oder andere Client-Fehler gelten.

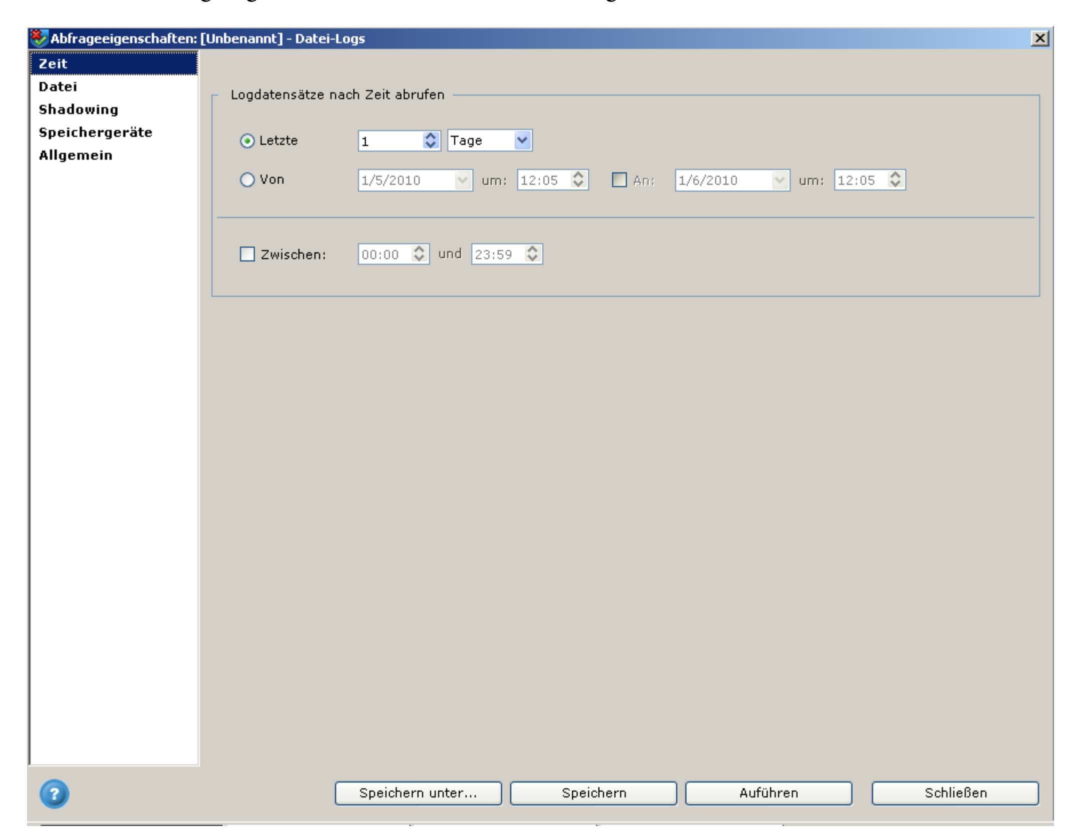
**Hinweis:** Die Interaktion der Auswahlmöglichkeiten auf der Registerkarte *Administration* erfolgt über die Boolesche "ODER"-Anweisung. Das bedeutet, dass Datensätze, die einem beliebigen der auf dieser Registerkarte festgelegten Kriterien entsprechen, in der Log-Tabelle angezeigt werden.

## 5.5.3 Definieren einer neuen Datei-Log-Abfrage

Mit File-Log-Abfragen können Sie die Log-Tabelle nach verschiedenen Eigenschaften filtern. Sie enthalten die folgenden Registerkarten: Zeit, Datei, Shadowing, Speichergeräte und Allgemein. Wenn die Option der Inhaltsprüfung aktiviert ist, ist auch die Registerkarte *Inhaltsprüfung* verfügbar.

### 5.5.3.1 Zeiteigenschaften – Datei-Logs

Die Zeit-Abfrageeigenschaften werden auf der Registerkarte *Zeit* definiert:



#### 5.5.3.1.1 Definieren von Zeiteigenschaften – Datei-Logs

Auf der Registerkarte Zeit definieren Sie den Zeitrahmen für die anzuzeigenden Datensätze. Unabhängig von anderen Abfragedefinitionen werden die Datensätze in der Log-Tabelle den von Ihnen hier festgelegten Zeitkriterien entsprechen.

**So definieren Sie Zeiteigenschaften:**

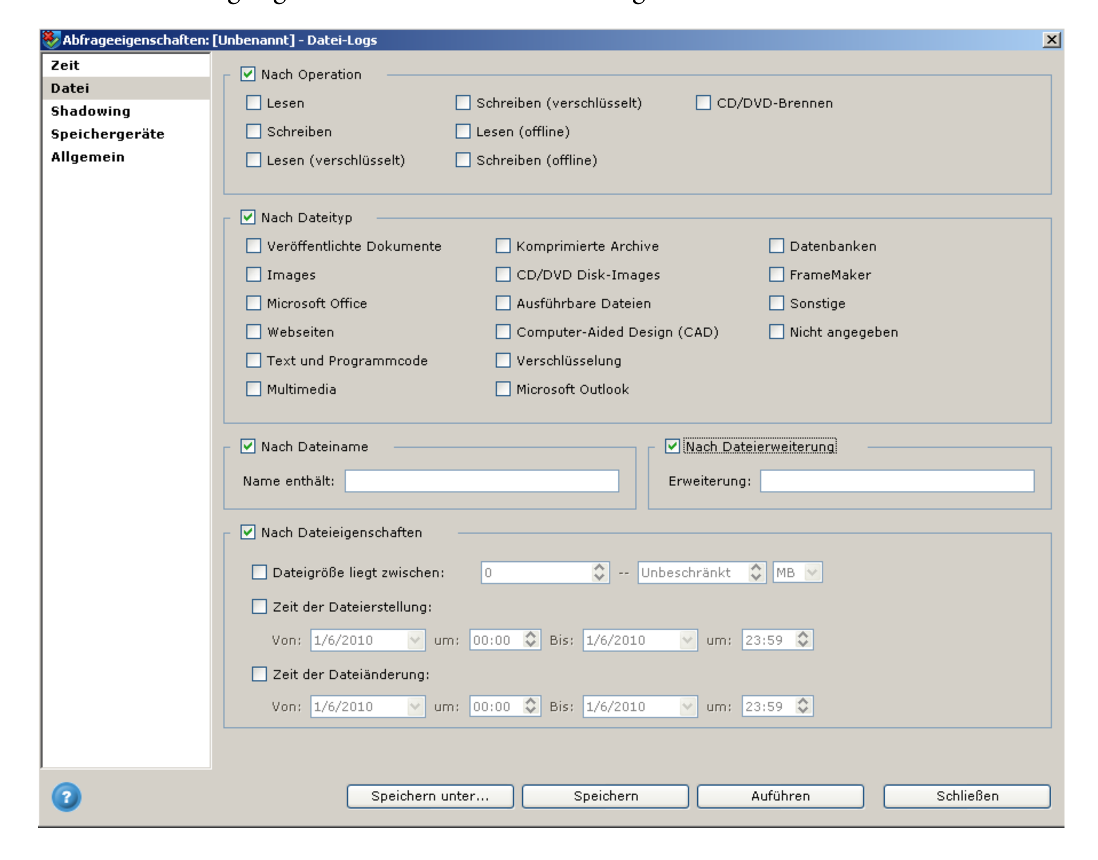
Geben Sie auf der Registerkarte *Zeit* den gewünschten Zeitrahmen für Logdatensätze ein. Die folgenden Optionen sind verfügbar:

- Klicken Sie auf die Optionsschaltfläche **Letzte**, um einen Zeitraum relativ zum aktuellen Tag auszuwählen. Wenn Sie möchten, geben Sie ein Zeitfenster für die Tage im ausgewählten Zeitraum an, indem Sie das Kontrollkästchen **Zwischen** markieren.
- Klicken Sie auf die Optionsschaltfläche **Von**, um ein definitives Datum und eine definitive Zeit auszuwählen, ab wann Datensätze angezeigt werden sollen. Markieren Sie das Kontrollkästchen **Bis**, wenn Sie ein definitives Enddatum und eine definitive Endzeit festlegen möchten, so dass nur Datensätze angezeigt werden, die zwischen die **Von**- und **Bis**-Zeit fallen.

Als Ergebnis werden nur Datensätze in der Log-Tabelle angezeigt, die Ihrer Auswahl entsprechen.

### 5.5.3.2 Dateieigenschaften – Datei-Logs

Die Datei-Abfrageeigenschaften werden auf der Registerkarte *Datei* definiert:



#### 5.5.3.2.1 Definieren von Dateieigenschaften – File-Logs

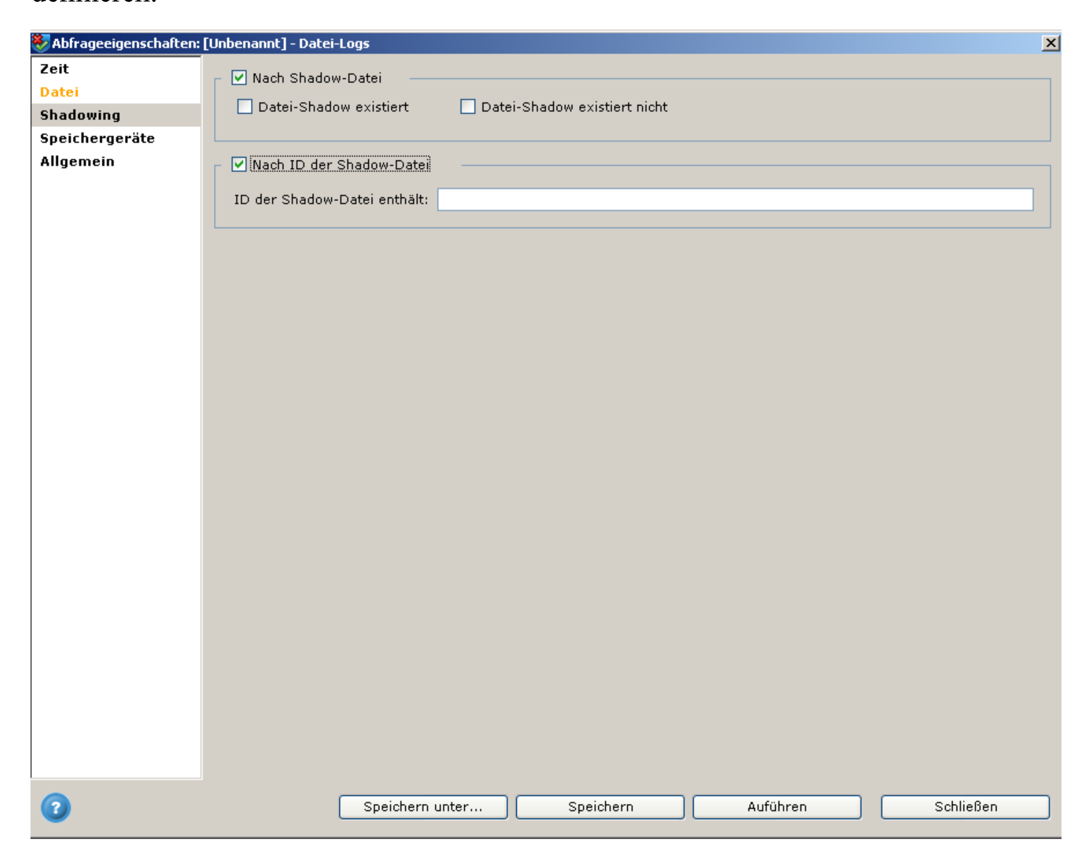
Auf der Registerkarte *Datei* definieren Sie die anzuzeigenden Logdatensätze bezüglich ihrer Dateiattribute. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen.

Im Folgenden werden die Abschnitte dieser Registerkarte beschrieben:

- **Nach Operation –** Markieren Sie dieses Kontrollkästchen, wenn die Log-Tabelle Logs für Dateien anzeigen soll, die von Geräten gelesen, auf Geräte geschrieben, von verschlüsselten Geräten gelesen oder auf verschlüsselte Geräte geschrieben wurden. Aktivieren Sie dann das entsprechende Kontrollkästchen für die gewünschte Operation (Sie können mehrere Optionen auswählen). Wenn Sie das Kontrollkästchen **Nach Operation** deaktiviert lassen, werden Logs für alle Operationen in die Log-Tabelle aufgenommen.
- **Nach Dateityp –** Markieren Sie dieses Kontrollkästchen, wenn Sie in der Log-Tabelle nur Logs für bestimmte Dateitypen anzeigen möchten. Aktivieren Sie dann das entsprechende Kontrollkästchen für den gewünschten Typ (Sie können mehrere Optionen auswählen). Wenn Sie das Kontrollkästchen **Nach Dateityp** deaktiviert lassen, werden Logs für alle Dateitypen in die Log-Tabelle aufgenommen.
- **Nach Dateiname –** Markieren Sie dieses Kontrollkästchen, wenn die Log-Tabelle nur Logs für Dateien enthalten soll, deren Name eine bestimmte Zeichenfolge enthält. Geben Sie die Zeichenfolge im Feld **Name enthält** ein.
- **Nach Dateierweiterung –** Markieren Sie dieses Kontrollkästchen, wenn die Log-Tabelle nur Logs für Dateien eines bestimmten Typs nach ihrer Dateierweiterung enthalten sollt. Geben Sie dann die Dateierweiterung im Feld **Erweiterung** ein. Sie können mehrere Dateierweiterungen angeben. Trennen Sie diese mit Semikolon oder Doppelpunkt.
- **Nach Dateieigenschaften –** Klicken Sie auf dieses Kontrollkästchen, wenn die Log-Tabelle nur Dateien enthalten soll, die über die in diesem Abschnitt angegebenen Eigenschaften verfügen – **Dateigröße**, **Zeit der Dateierstellung** oder **Zeit der Dateiänderung**. Markieren Sie das gewünschte Kontrollkästchen für jede der Eigenschaften, und geben Sie bei Bedarf die Parameter an.

### 5.5.3.3 Shadowing-Eigenschaften – Datei-Logs

Auf der Registerkarte *Shadowing* können Sie Abfrageeigenschaften hinsichtlich Shadow-Dateien definieren:



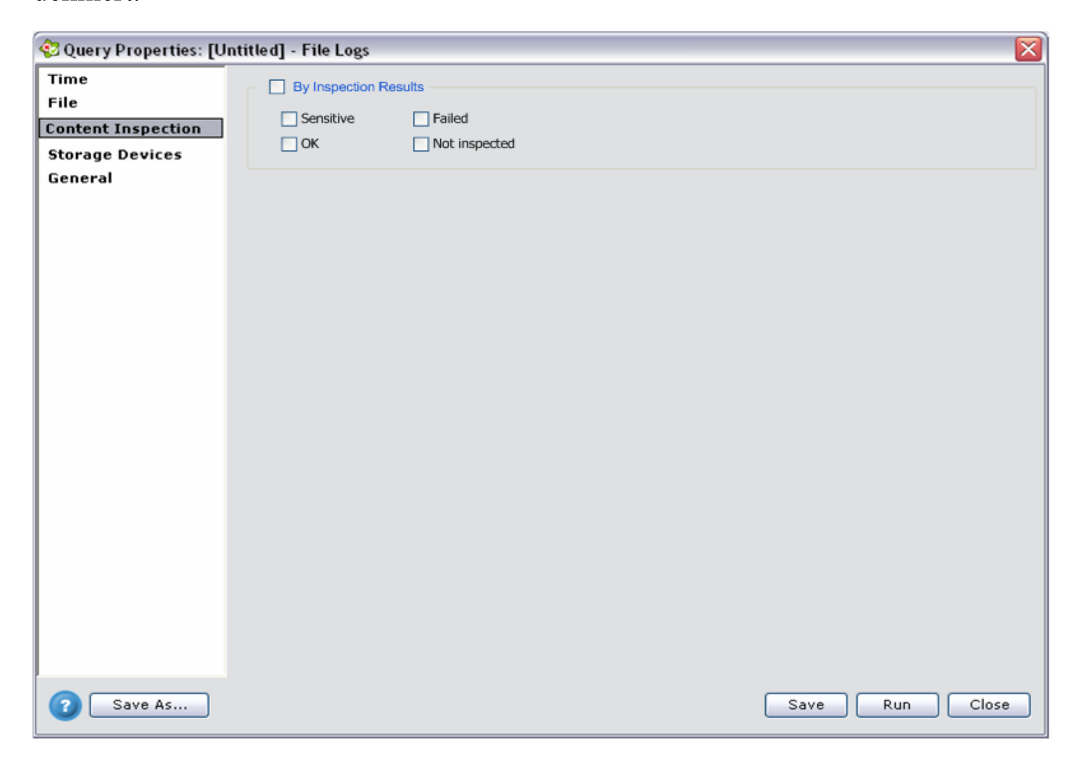

#### 5.5.3.3.1 Definieren von Shadowing-Eigenschaften – Datei-Logs

Im Folgenden werden die Abschnitte dieser Registerkarte beschrieben:

- **Nach Shadow-Datei –** In diesem Abschnitt geben Sie an, dass die in den Abfrageergebnissen aufgeführten Logdateien davon abhängen, ob eine Shadow-Datei für die protokollierte Datei erstellt wurde oder nicht.
  - Markieren Sie das Kontrollkästchen **Datei-Shadow existiert**, um anzugeben, dass die Logdateien in den Abfrageergebnissen die Logs von kopierten Shadow-Dateien enthalten. Diese Logs zeigen die tatsächlich kopierten Dateien an.
  - Markieren Sie das Kontrollkästchen **Datei-Shadow existiert nicht**, um anzugeben, dass **die** Logdateien in den Abfrageergebnissen die Logs von Dateien enthalten, die nicht kopiert wurden.
- **Nach ID der Shadow-Datei –** In diesem Abschnitt geben Sie die genaue ID der Shadow-Datei an, die in den Abfrageergebnissen gezeigt werden soll. Geben Sie im Feld **ID der Shadow-Datei enthält** die Logdatei-ID ganz oder teilweise an. Diese Logdatei-ID kann in einer Alarmmeldung enthalten sein, die beim Erstellen der Shadow-Kopie einer Datei gesendet wurde.

### 5.5.3.4 Inhaltsprüfungseigenschaften – Datei-Logs

Die Inhaltsprüfungs-Abfrageeigenschaften werden auf der Registerkarte *Content Inspection* definiert:



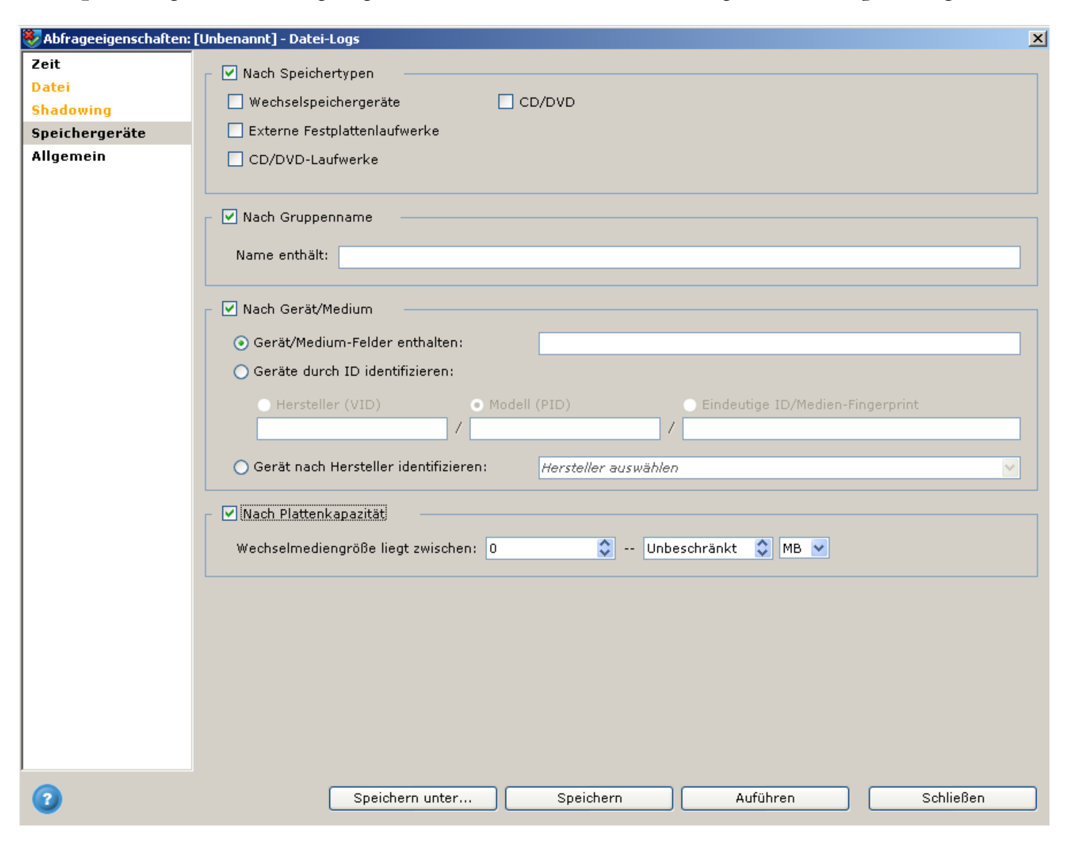

**Hinweis:** Diese Registerkarte wird nur dann angezeigt, wenn die Option der Inhaltsprüfung aktiviert ist.

#### 5.5.3.4.1 Definieren von Inhaltsprüfungseigenschaften

Hier definieren Sie die anzuzeigenden Logdatensätze bezüglich der Ergebnisse ihrer Inhaltsprüfung. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen.

### 5.5.3.5 Speichergeräteeigenschaften – Datei-Logs

Die Speichergeräte-Abfrageeigenschaften werden auf der Registerkarte *Speichergeräte* definiert:




#### 5.5.3.5.1 Definieren von Speichergeräteeigenschaften – Datei-Logs

Auf der Registerkarte *Speichergeräte* definieren Sie die anzuzeigenden Logdatensätze bezüglich ihrer Speichergeräteattribute. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen.

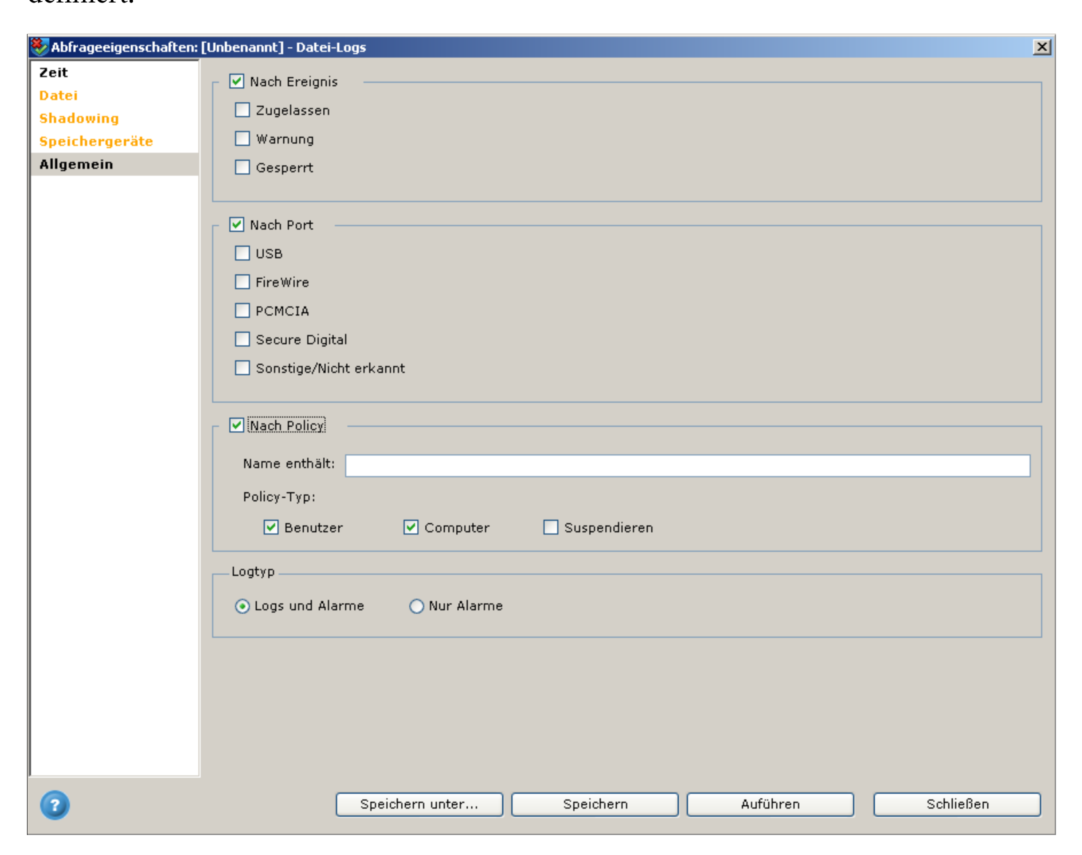
Im Folgenden werden die Abschnitte dieser Registerkarte beschrieben:

- **Nach Speichertypen** – In diesem Abschnitt können Sie den Speichergerätetyp (einschließlich CD/DVD-Medien) festlegen, der in die Log-Tabelle aufgenommen werden soll (Sie können mehrere Typen auswählen). Wenn Sie diesen Abschnitt nicht auswählen, werden die Datensätze unabhängig von dem Speichergerätetyp, für den sie gelten, angezeigt.
- **Nach Gruppenname** – In diesem Abschnitt können Sie den Namen (ganz oder teilweise) der Speichergerätegruppe eingeben, die in die Log-Tabelle aufgenommen werden soll. Es werden nur Geräte angezeigt, die zu diesen Gruppen gehören. Wenn Sie keinen Gruppennamen eingeben, werden in der Log-Tabelle Datensätze unabhängig von der Gruppe angezeigt, der sie angehören.
- **Nach Gerät/Medium** – In diesem Abschnitt können Sie die Speichergeräte oder CD/DVD auswählen, die in die Log-Tabelle aufgenommen werden sollen. Sie können sie auswählen, indem Sie den Gerätenamen (ganz oder teilweise oder ein anderes Textfeld. oder Vendor-ID, Modell oder Distinct-ID, oder – bei CD/DVD – ihren Fingerprint eingeben. Wenn Sie in diesem Abschnitt keine Auswahl treffen, werden Datensätze für alle Geräte, die zu den Speichergerätetypen gehören, angezeigt.

- **Nach Plattenkapazität –** Wenn Sie Nach Speichertypen (siehe oben), **Removable Storage Devices** oder **External Hard Disks** wählen, können Sie in diesem Abschnitt den Bereich der Mediengröße definieren, der in die Log-Tabelle aufgenommen werden soll. Wenn Sie keine auswählen, werden in der Log-Tabelle Datensätze für Speichergeräte unabhängig von ihrer Kapazitätsgröße angezeigt.

### 5.5.3.6 Allgemeine Eigenschaften – Datei-Logs

Die allgemeinen Abfrageeigenschaften werden auf der unten gezeigten Registerkarte *Allgemein* definiert:




#### 5.5.3.6.1 Definieren von allgemeinen Eigenschaften – Datei-Logs

Auf der Registerkarte *Allgemein* definieren Sie die anzuzeigenden Logdatensätze bezüglich ihrer Port- und Policy-Attribute. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen. Im Folgenden werden die Abschnitte dieser Registerkarte beschrieben:

- **Nach Ereignis –** Markieren Sie dieses Kontrollkästchen, wenn Sie im Log nur Dateien anzeigen möchten, die mit einem bestimmten Kontrollereignis verknüpft sind. Markieren Sie in diesem Fall das entsprechende Kontrollkästchen für die Ereignisse, die aufgenommen werden sollen.
- **Nach Port –** Markieren Sie dieses Kontrollkästchen, wenn Sie im Log nur Dateien anzeigen möchten, die mit einem bestimmten Port verknüpft sind. Markieren Sie in diesem Fall das entsprechende Kontrollkästchen für die Ports, die aufgenommen werden sollen.

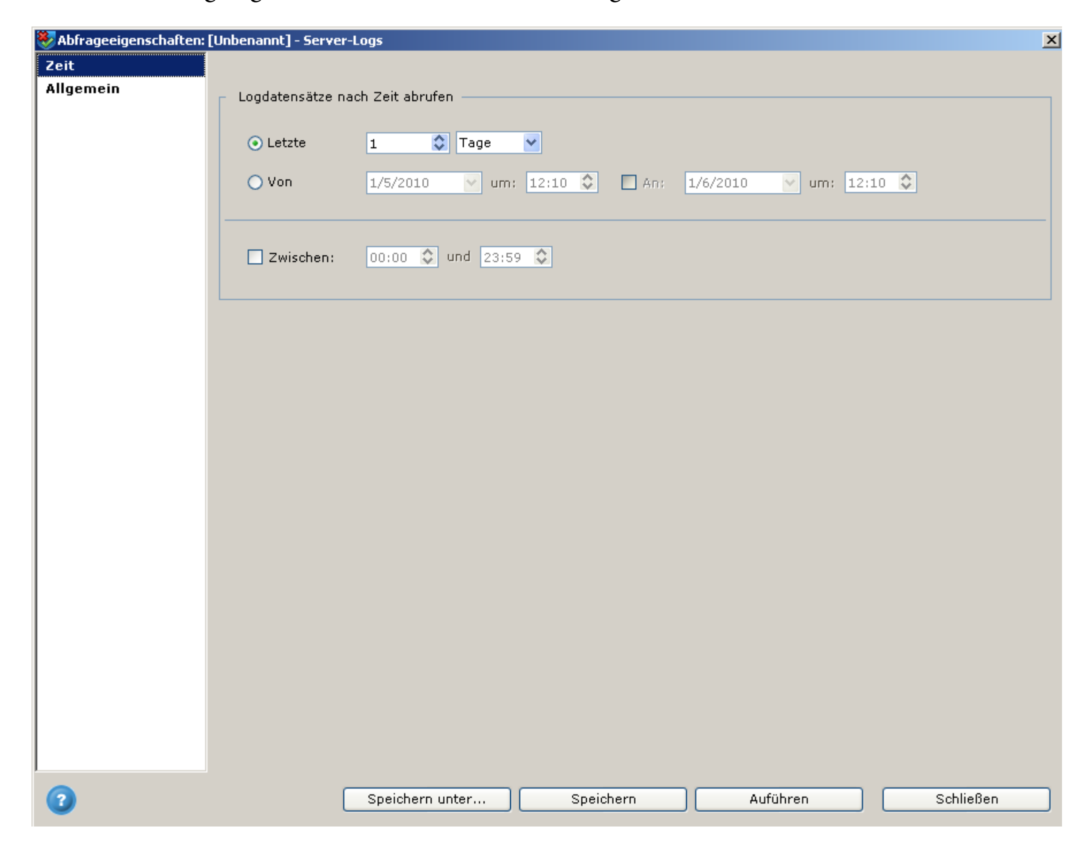
- **Nach Policy –** In diesem Abschnitt können Sie den Namen (ganz oder teilweise) der Policy bzw. Policies eingeben, die mit den Datensätzen in der Log-Tabelle verknüpft werden sollen. Es werden nur Policies angezeigt, deren Name den von Ihnen eingegebenen Text enthält. Wenn Sie diesen Abschnitt auswählen, werden in der Log-Tabelle Datensätze unabhängig von der Policy, mit der sie verknüpft sind, angezeigt.
  Wenn Sie diesen Abschnitt auswählen, müssen Sie einen der Policy-Typen auswählen.
- **Logtyp –** In diesem Abschnitt können Sie wählen, ob die Log-Tabelle Logs und Alarme oder nur Alarme anzeigen soll (abhängig davon, wie Sie die Log- und Alarmeinstellungen im Fenster *Dateikontrolle* Ihrer Policy festgelegt haben, kann bei der Anzeige von Logs und Alarmen eine sehr große Anzahl an Datensätzen generiert werden). Klicken Sie auf die gewünschte Optionsschaltfläche.

## 5.5.4 Definieren einer neuen Server-Log-Abfrage

Mit Server-Log-Abfragen können Sie die Log-Tabelle des Management Servers nach verschiedenen Eigenschaften filtern, die für Server-Ereignisse relevant sind. Hierzu gehören die Registerkarte *Zeit* und *Allgemein*.

### 5.5.4.1 Zeiteigenschaften – Server-Logs

Die Zeit-Abfrageeigenschaften werden auf der Registerkarte *Zeit* definiert:



#### 5.5.4.1.1 Definieren von Zeiteigenschaften – Server-Logs

Auf der Registerkarte *Zeit* definieren Sie den Zeitrahmen für die anzuzeigenden Datensätze. Unabhängig von anderen Abfragedefinitionen werden die Datensätze in der Log-Tabelle den von Ihnen hier festgelegten Zeitkriterien entsprechen.

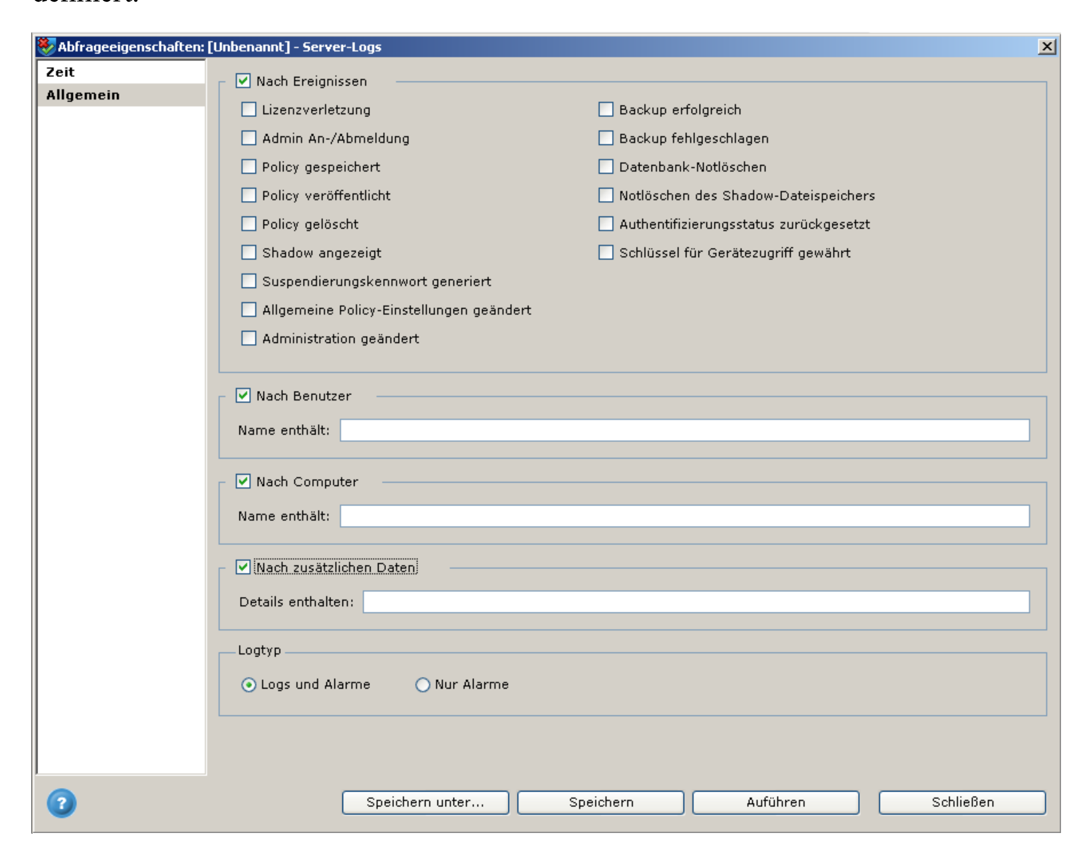
**So definieren Sie Zeiteigenschaften:**

Geben Sie auf der Registerkarte *Zeit* den gewünschten Zeitrahmen für Logdatensätze ein. Die folgenden Optionen sind verfügbar:

- Klicken Sie auf die Optionsschaltfläche **Letzte**, um einen Zeitraum relativ zum aktuellen Tag auszuwählen. Wenn Sie möchten, geben Sie ein Zeitfenster für die Tage im ausgewählten Zeitraum an, indem Sie das Kontrollkästchen **Zwischen** markieren.
- Klicken Sie auf die Optionsschaltfläche **Von**, um ein definitives Datum und eine definitive Zeit auszuwählen, ab wann Datensätze angezeigt werden sollen. Markieren Sie das Kontrollkästchen **Bis**, wenn Sie ein definitives Enddatum und eine definitive Endzeit festlegen möchten, so dass nur Datensätze angezeigt werden, die zwischen die **Von**- und **Bis**-Zeit fallen. Als Ergebnis werden nur Datensätze in der Log-Tabelle angezeigt, die Ihrer Auswahl entsprechen.

### 5.5.4.2 Allgemeine Eigenschaften – Server-Logs

Die allgemeinen Abfrageeigenschaften werden auf der unten gezeigten Registerkarte *Allgemein* definiert:



#### 5.5.4.2.1 Definieren von allgemeinen Abfrageeigenschaften – Server-Logs

Auf der Registerkarte *Allgemein* definieren Sie die anzuzeigenden Logdatensätze bezüglich ihrer Attribute. In der Log-Tabelle erscheinen nur Datensätze, die den von Ihnen hier festgelegten Kriterien entsprechen.

Im Folgenden werden die Abschnitte dieser Registerkarte beschrieben:

- **Nach Ereignissen –** Klicken Sie auf dieses Kontrollkästchen, wenn das Log Datensätze anzeigen soll, die zu bestimmten Server-Ereignissen gehören. Wählen Sie die gewünschten Ereignisse durch Aktivieren des entsprechenden Kontrollkästchens aus.
- **Nach Benutzer**- Klicken Sie auf dieses Kontrollkästchen, wenn die Log-Tabelle Datensätze enthalten soll, die zu einem bestimmten Administrator gehören, dessen Name eine bestimmte Zeichenfolge enthält. In diesem Fall geben Sie die gewünschte Zeichenfolge im Feld *Name enthält* ein.
- **Nach Computer**- Klicken Sie auf dieses Kontrollkästchen, wenn die Log-Tabelle Datensätze enthalten soll, die zu einer bestimmten SafeGuard PortProtector Management Console gehören, deren Name eine bestimmte Zeichenfolge enthält. In diesem Fall geben Sie die gewünschte Zeichenfolge im Feld *Name enthält* ein.
- **Nach zusätzlichen Daten –** Klicken Sie auf dieses Kontrollkästchen, wenn die Log-Tabelle Datensätze enthalten soll, die in ihrem Details-Feld eine bestimmte Zeichenfolge enthalten. In diesem Fall geben Sie die gewünschte Zeichenfolge im Feld *Details enthalten* ein.
- **Logtyp –** In diesem Abschnitt geben Sie an, ob die Log-Tabelle Logs und Alarme oder nur Alarme anzeigen soll.

### 5.5.5 Ausführen einer neuen Abfrage

Sie können bei Bedarf eine neue Abfrage direkt aus dem Fenster *Abfrageeigenschaften* heraus ausführen.

**So führen Sie eine neue Abfrage aus:**

Klicken Sie im Fenster *Abfrageeigenschaften* nach dem Speichern der Abfrage auf **Ausführen**. Die Abfrage wird aktiviert und die Log-Tabelle zeigt die Datensätze an, die Ihren Abfragekriterien entsprechen.

**Hinweis:** Wenn Sie die neue Abfrage vor dem Ausführen nicht speichern und benennen, können Sie sie später, wenn sie nicht mehr aktiv ist, nicht mehr verwenden.

### 5.5.6 Speichern einer neuen Abfrage

Nachdem Sie die Definition der Abfrage abgeschlossen haben, können Sie sie für zukünftige, wiederholte Nutzung speichern.

**So speichern Sie eine neue Abfrage:**

1. Klicken Sie im Fenster *Abfrageeigenschaften* auf **Speichern**. Das Fenster *Abfrage speichern* wird angezeigt.
2. Geben Sie im Fenster *Abbfrage speichern* den gewünschten Abfragenamen (zwingend erforderlich) und eine Beschreibung (optional) ein, und klicken Sie auf **OK**. Die Abfrage wird gespeichert, und ab diesem Zeitpunkt können Sie sie im Symbolleistenmenü Abfrage auswählen.

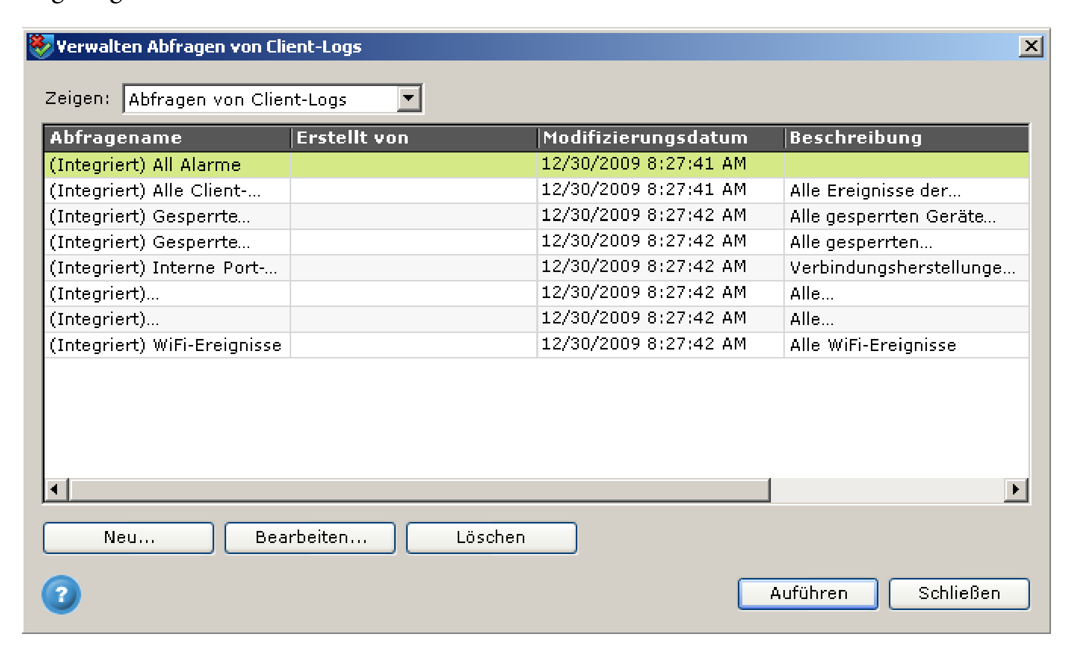
## 5.5.7 Verwalten von Abfragen

**So öffnen Sie das Fenster Verwalten Abfragen:**

Klicken Sie in der Symbolleiste auf die Schaltfläche **Abfragen verwalten** .

ODER

Klicken Sie im Menü *Datei* auf die Option **Abfragen.** Der Fenster *Verwalten Abfragen* wird angezeigt:




### 5.5.7.1 Optionen der Abfrageverwaltung

Im Fenster *Verwalten Abfragen* werden die integrierten Abfragen (in *Integrierte Abfragen* beschrieben) sowie Ihre gespeicherten Abfragen für den ausgewählten Abfragetyp (Client-Logs, Datei-Logs oder Server-Logs) angezeigt. In diesem Fenster können Sie folgende Aktivitäten ausführen:

- Definieren neuer Abfragen, in *Erstellen einer Abfrage* erläutert.
- Bearbeiten vorhandener Abfragen, in *Bearbeiten einer Abfrage* erläutert.
- Löschen von Abfragen, in *Löschen einer Abfrage* erläutert.
- Umbenennen von Abfragen, in *Umbenennen einer Abfrage* erläutert.
- Ausführen von Abfragen, in *Ausführen einer zuvor definierten Abfrage* erläutert.

Standardmäßig werden in diesem Fenster aller Abfragen für den aktiven Logtyp (Client-Log, Server-Log oder File-Log) angezeigt. Sie können bei Bedarf Abfragen für einen anderen Logtyp anzeigen und verwalten.

**So ändern Sie den Abfrage-Logtyp:**

Klicken Sie im Fenster *Verwalten Abfragen* auf das Menü **Zeigen** und wählen Sie den gewünschten Logtyp für die zu verwaltenden Abfragen. Das Fenster zeigt jetzt Abfragen für den von Ihnen gewählten Logtyp.

#### 5.5.7.2 Erstellen einer Abfrage

Das Erstellen einer neuen Abfrage wird detailliert in *Abfragen* erläutert. Das Fenster *Abfrageeigenschaften*, in dem Sie die Eigenschaften der neuen Abfrage definieren, kann auch aus dem Fenster *Verwalten Abfrage* heraus geöffnet werden.

#### 5.5.7.3 Bearbeiten einer Abfrage

Eine Abfrage kann bearbeitet werden, wenn ihre Eigenschaften geändert werden müssen oder Sie sie als Vorlage bei der Erstellung einer neuen Abfrage verwenden möchten.

**So bearbeiten Sie eine Abfrage:**

1 Klicken Sie in der Symbolleiste auf die Schaltfläche **Bearbeiten** . Das Fenster *Abfrageeigenschaften* wird angezeigt.

2 Nehmen Sie die gewünschten Änderungen vor.

ODER

1 Wählen Sie im Fenster *Verwalten Abfragen* die zu bearbeitende Abfrage aus der Abfrageliste aus.

2 Klicken Sie auf **Bearbeiten**. Das Fenster *Abfrageeigenschaften* wird angezeigt.

3 Nehmen Sie die gewünschten Änderungen vor.

ODER

1 Klicken Sie im Fenster *Verwalten Abfragen* in der Abfrageliste mit der rechten Maustaste auf die zu bearbeitende Abfrage.

2 Wählen Sie im Kontextmenü die Option **Bearbeiten**. Das Fenster *Abfrageeigenschaften* wird angezeigt.

3 Nehmen Sie die gewünschten Änderungen vor.

**So speichern Sie eine bearbeitete Abfrage:**

1 Speichern einer Abfrage unter ihrem Namen:

2 Klicken Sie auf Speichern, um die geänderte Abfrage unter ihrem bestehenden Namen zu speichern.

3 Speichern der geänderten Abfrage als eine neue Abfrage:

4 Klicken Sie auf **Speichern unter**. Das Fenster *Abfrage speichern* wird angezeigt.

5 Geben Sie im Fenster *Abfrage speichern* den gewünschten Abfragenamen (zwingend erforderlich) und eine Beschreibung (optional) ein, und klicken Sie auf **OK**. Die Abfrage wird gespeichert, und ab diesem Zeitpunkt können Sie sie im Symbolleistenmenü Abfrage auswählen.

#### 5.5.7.4 Löschen einer Abfrage

Sie können Abfragen löschen, für die Sie keine Verwendung mehr haben.

**So löschen Sie eine Abfrage:**

1. Wählen Sie im Fenster *Manage Queries* die zu löschende Abfrage aus der Abfrageliste aus (mit Hilfe der **Strg**- bzw. **Umschalttaste** können Sie mehrere zu löschende Abfragen selektieren).
2. Klicken Sie auf **Löschen.** Ein Bestätigungsfenster wird angezeigt.
3. Klicken Sie auf **Ja**, um die Abfrage(n) zu löschen, oder auf **Nein**, um den Vorgang abzubrechen.

ODER

1. Klicken Sie in der Abfrageliste mit der rechten Maustaste auf die zu löschende Abfrage (vor dem Rechtsklicken können Sie die **Strg**- bzw. **Umschalttaste** drücken, um mehrere zu löschende Abfragen zu selektieren).
2. Wählen Sie im Kontextmenü die Option **Löschen**. Ein Bestätigungsfenster wird angezeigt.
3. Klicken Sie auf **Ja**, um die Abfrage(n) zu löschen, oder auf **Nein**, um den Vorgang abzubrechen.

#### 5.5.7.5 Umbenennen einer Abfrage

Sie können eine Abfrage umbenennen.

**So benennen Sie eine Abfrage um:**

1. Wählen Sie im Fenster *Verwalten Abfragen* die umzubenennende Abfrage aus der Abfrageliste aus.
2. Klicken Sie auf das Feld **Name.** Der Abfragename ist jetzt selektiert und kann bearbeitet werden.

### 5.5.8 Ausführen einer zuvor definierten Abfrage

Die Ausführung einer Abfrage bezieht sich auf die von Ihnen definierten Abfragekriterien. Zusammen mit der Auswahl in der Organisationsstruktur wird dadurch bestimmt, welche Datensätze in der Log-Tabelle erscheinen. Sie können eine zuvor definierte Abfrage auf verschiedene Weise ausführen: über die Symbolleiste, im Fenster *Verwalten Abfragen* über die Schaltfläche **Ausführen**, im Fenster *Verwalten Abfragen* über das Kontextmenü, oder im Fenster *Verwalten Abfragen* durch Doppelklicken auf die Abfrage.

**So führen Sie eine zuvor definierte Abfrage über die Symbolleiste aus:**

Klicken Sie in der Symbolleiste auf das Menü **Abfrage** und wählen Sie die auszuführende Abfrage aus. Die Abfrage wird für die Log-Tabelle angewandt.

**So führen Sie eine zuvor definierte Abfrage über das Fenster *Verwalten Abfragen* aus:**

1 Wählen Sie im Fenster *Manage Queries* die auszuführende Abfrage aus der Abfrageliste aus.

2 Klicken Sie auf **Ausführen.** Die Abfrage wird für die Log-Tabelle angewandt.

ODER

1 Klicken Sie in der Abfrageliste mit der rechten Maustaste auf die auszuführende Abfrage.

2 Klicken Sie im Kontextmenü auf **Ausführen**. Die Abfrage wird auf die Log-Tabelle angewandt.

ODER

Doppelklicken Sie in der Abfrageliste auf die auszuführende Abfrage. Die Abfrage wird auf die Log-Tabelle angewandt.

**Hinweis:** Wenn die auszuführende Abfrage zu einem anderen Typ als zur aktiven Log-Tabelle gehört (wenn z. B. die aktive Log-Tabelle Client-Logs zeigt und die Abfrage für Server-Logs gilt), wird ein neues, zusätzliches Log-Fenster geöffnet, in dem die neue Log-Tabelle angezeigt wird.

### 5.5.9 Aufheben der Abfrage

Wenn Sie die Anwendung der Abfrage aufheben und wieder zur Standardanzeige der Log-Tabelle zurückkehren möchten, wählen Sie All Logs im Menü *Abfragen*. Die Log-Tabelle zeigt jetzt alle Logs.

## 5.6 Optionen für aktives Fenster

Das aktive Fenster kann dupliziert, gelöst und geschlossen werden. Diese Optionen sind in *Optionen für aktives* Fensterim Kapitel *Erste Schritte*, beschrieben.

## 5.7 Erfassen von Logs

Mit dieser Option können Sie Logs von einem geschützten Computer außerhalb der geplanten Erfassungszeiten erfassen, um die aktuellsten Informationen zu sehen. Bei Aktivierung dieser Funktion werden alle Logtypen erfasst. Anleitungen hierzu finden Sie in *Abrufen der aktuellesten Informationen* von einem Client im Kapitel *Verwalten von Clients.*

## 5.8 Verfolgen des Fortschritts von Client-Tasks

Wenn die Anwendung Tasks ausführt (wie etwa das Erfassen von Logs oder das Aktualisieren von Policies), können Sie den Verlauf dieser Tasks anzeigen lassen. Anleitungen hierzu finden Sie in Verfolgen des Fortschritts von Client-Tasks im Kapitel *Verwalten von Clients.*

## 5.9 Struktur der Log-Tabellen

Im Folgenden werden die Spalten der Log-Tabellen beschrieben:

- *Struktur des Client-Logs* beschreibt die Spalten in der Client-Log-Tabelle.
- *Struktur des Datei-Logs* beschreibt die Spalten in der File-Log-Tabelle.
- *Struktur des Server-Logs* beschreibt die Spalten in der Server-Log-Tabelle.

### 5.9.1 Struktur des Client-Logs

Im Folgenden werden die Spalten der Client-Log-Tabelle beschrieben:

| Spalte | Beschreibung |
|---|---|
| **Log Type** | Gibt an, ob es sich bei dem Datensatz um ein Log oder einen Alarm handelt. |
| **Scope** | Gibt den Umfang an, auf den sich das Ereignis bezieht (z. B. Port, Speicher, Admin, Manipulation). |
| **Time** | Zeigt die Zeit des Ereignisses als Management Console-Zeit an. |
| **Computer** | Zeigt den vollständigen Namen (einschließlich der Domänenendung) des Computers an, für den das Ereignis gilt. |
| **User** | Zeigt den Namen des Benutzers an, für den das Ereignis gilt. |

| Spalte | Beschreibung |
|---|---|
| **Event** | ▪ Zeigt das Ereignis an. Mögliche Werte sind:<br>▪ Port restricted<br>▪ Allowed<br>▪ Encrypted<br>▪ Read Only<br>▪ Blocked<br>▪ Disconnected<br>▪ Missing Logs (tampering attempt)<br>▪ Process Killed (tampering attempt)<br>▪ Invalid Files (tampering attempt)<br>▪ Invalid Policy (tampering attempt)<br>▪ Install<br>▪ Uninstall<br>▪ Uninstall Failed<br>▪ Wrong Admin Password<br>▪ Suspension Password Generated<br>▪ Suspended (User)<br>▪ Suspended (Admin)<br>▪ Suspension Failed<br>▪ Wieder aufgenommen (d. h., fortgesetzter Schutz nach Suspendierung)<br>▪ Set Offline Access Password<br>▪ Policy aktualisiert<br>▪ Other Client Errors<br>▪ Zugriffskennwort geändert<br>▪ Falsches Deinstallationskennwort<br>▪ Nicht authentifizierter Zugriff |
| **Port** | Zeigt den Porttyp des Ports, der mit dem Ereignis verknüpft ist. |
| **Device Type** | Zeigt den Gerätetyp des Geräts, das mit dem Ereignis verknüpft ist. |

| Spalte | Beschreibung |
|---|---|
| **Device Description** | Zeigt die Beschreibung des Geräts, das mit dem Ereignis verknüpft ist. Die Gerätebeschreibung wird vom Gerät entnommen. |
| **Device Info** | Zeigt die Gerätedaten des Geräts an, das mit dem Dateiereignis verknüpft ist. Die Gerätedaten werden vom Gerät entnommen. |
| **Group** | Zeigt den Namen der Gruppe der freigegebenen Geräte, Speichergeräte oder WiFi-Verbindungen an, zu der das mit diesem Ereignis verknüpfte Gerät bzw. die Verbindung gehört. |
| **Policy Type** | Gibt an, ob es sich bei der zugewiesenen Policy um eine Computer-Policy oder eine Benutzer-Policy handelt. |
| **Policy** | Zeigt den Namen der Policy an, die auf dem meldenden Client angewandt ist. Wenn auf diesem Client Policies zusammengeführt sind, werden alle zusammengeführten Policies aufgeführt. |
| **Vendor** | Zeigt den Gerätehersteller an. |
| **Model** | Zeigt das Gerätemodell an. |
| **Distinct ID** | Zeigt die eindeutige ID des spezifischen Geräts an, sofern verfügbar. |
| **Details** | Zeigt ggf. Zusatzinformationen an, z. B. Verschlüsselungstyp (für WiFi-Netzwerkverschlüsselung), Name der manipulierten Datei etc. |
| **Client Local** | Zeigt die Ereigniszeit als lokale Zeit des Clients, der das Ereignis gemeldet hat. |
| **DB Insert** | Zeigt den Zeitpunkt als Management Console-Zeit an, an dem das Ereignis in die Datenbank eingetragen wurde. |
| **Sequence** | Jeder Client sendet seine Logs mit einer Folgenummer, was dazu beiträgt, fehlende Logs zu entdecken und über Log-Manipulationsversuche zu alarmieren. Sie können dies z. B. bei einem „Missing Log“-Ereignis für einen bestimmten Computer verwenden. |

### 5.9.2 Struktur des Datei-Logs

Im Folgenden werden die Spalten der File-Log-Tabelle beschrieben:

| Spalte | Beschreibung |
|---|---|
| **Log Type** | Gibt an, ob es sich bei dem Datensatz um ein Log oder einen Alarm handelt. |
| **Time** | Zeigt die Zeit des Ereignisses als Management Console-Zeit an. |
| **Computer** | Zeigt den vollständigen Namen (einschließlich der Domänenendung) des Computers an, für den das Ereignis gilt. |
| **User** | Zeigt den Namen des Benutzers an, für den das Ereignis gilt. |
| **Event** | Zeigt das Dateiereignis an. Mögliche Werte sindZugelassen:<br>▪ Warnung:<br>(Wenn die Inhaltsprüfung aktiviert ist und sensible Inhalte festgestellt werden.)<br>▪ Gesperrt<br>Wenn Sie gewählt haben, das Schreiben von Dateien zu sperren, wenn das Brennformat keine Protokollierung ermöglicht (siehe *Festlegen der Berechtigungen für CD/DVD* in *Kapitel 3, Definieren von Policies*), gibt diese Spalte an, dass das Schreiben gesperrt wurde. |
| **Operation** | Zeigt den Typ der ausgeführten Operation an. Mögliche Werte sind:<br>▪ Read<br>▪ Write<br>▪ Read (encrypted)<br>▪ Write (encrypted)<br>▪ Read (offline)<br>▪ Write (offline) |
| **File Type** | Zeigt den Namen des Dateityps an (z. B. Microsoft Word). |

| Spalte | Beschreibung |
|---|---|
| **Extension** | Zeigt die Dateierweiterung der protokollierten Datei. |
| **File Name** | Zeigt den Pfad und den Namen der protokollierten Datei. |
| **Shadow File** | Zeigt ein Kontrollhäkchen, wenn für diesen Logeintrag eine Shadow-Datei erstellt wurde. |
| **Shadow File ID** | Zeigt die eindeutige Datei-ID der Shadow-Datei an, die durch diesen Logeintrag im Datei-Shadow-Speicher dargestellt wird. Weitere Informationen zur Konfiguration des zentralen Datei-Shadow-Speichers finden Sie in *Schritt 15: Einstellungen für Datei-Shadowing definieren*. |
| **File Size** | Zeigt die Größe der protokollierten Datei in Bytes an. |
| **Created** | Diese Spalte zeigt das Datum und die Uhrzeit an, wann die protokollierte Datei erstellt wurde. |
| **Modified** | Zeigt das Datum und die Uhrzeit an, wann die protokollierte Datei modifiziert wurde. |
| **Inspect Results** | Diese Spalte wird nur dann angezeigt, wenn die Inhaltsprüfung durchgeführt wird; sie zeigt die Prüfergebnisse an. Mögliche Werte sind:<br>▪ Sensitive<br>▪ OK<br>▪ Failed<br>▪ leer (nicht geprüft) |
| **Inspect Time** | Diese Spalte wird nur dann angezeigt, wenn die Inhaltsprüfung durchgeführt wird; sie zeigt das Datum und die Uhrzeit der Prüfung an. |
| **Inspect Details** | Zeigt den Port an, der mit dem Dateiereignis verknüpft ist. |

| Spalte | Beschreibung |
|---|---|
| **Port** | Zeigt den Gerätetyp des Geräts an, das mit dem Dateiereignis verknüpft ist. |
| **Device Type** | Zeigt die Gerätebeschreibung des Geräts/Netzes an, das mit dem Dateiereignis verknüpft ist. |
| **Device Description/ Network** | Zeigt die Gerätedaten des Geräts an, das mit dem Dateiereignis verknüpft ist. |
| **Device Info** | Zeigt den Namen der Gruppe der freigegebenen Geräte, Speichergeräte oder WiFi-Verbindungen an, zu der das mit diesem Ereignis verknüpfte Gerät bzw. die Verbindung gehört. |
| **Group Name** | Gibt an, ob es sich bei der zugewiesenen Policy um eine Computer-Policy oder eine Benutzer-Policy handelt. |
| **Policy Type** | Zeigt den Namen der Policy an, die auf dem meldenden Client angewandt ist. Wenn auf diesem Client Policies zusammengeführt sind, werden alle zusammengeführten Policies aufgeführt. |
| **Policy** | Zeigt den Gerätehersteller an. |
| **Vendor** | Zeigt das Gerätemodell an. |
| **Model** | Zeigt die eindeutige ID des spezifischen Geräts an, sofern verfügbar. |
| **Distinct ID** | Zeigt ggf. weitere Details an. |
| **Details** | Zeigt die Ereigniszeit als Zeit des Clients, der das Ereignis gemeldet hat. |
| **Client Local** | Zeigt den Zeitpunkt als Management Console-Zeit an, zu dem der Management Server das Ereignis empfangen hat. |

| Spalte | Beschreibung |
|---|---|
| **DB Insert** | Zeigt den Port an, der mit dem Dateiereignis verknüpft ist. |
| **Sequence** | Jeder Client sendet seine Logs mit einer Folgenummer, was dazu beiträgt, fehlende Logs zu entdecken und über Log-Manipulationsversuche zu alarmieren. Sie können dies z. B. bei einem "Fehlende Logs"-Ereignis für einen bestimmten Computer verwenden. |

## 5.9.3 Struktur des Server-Logs

Im Folgenden werden die Spalten der Server-Log-Tabelle beschrieben:

| Spalte | Beschreibung |
|---|---|
| **Logtyp** | Gibt an, ob es sich bei dem Datensatz um ein Log oder einen Alarm handelt. |
| **Scope** | Gibt den Umfang an, auf den sich das Ereignis bezieht (z. B. Admin, Lizenz). |
| **DB Insert** | Zeigt die Zeit des Ereignisses als lokale Management Console-Zeit an. |
| **Computer** | Zeigt den Namen der Management Console an, für die das Ereignis gilt. |
| **User** | Zeigt den Namen des Administrators an, für den das Ereignis gilt. |

| Spalte | Beschreibung |
|---|---|
| **Event** | Diese Spalte zeigt den Ereignistyp an. Mögliche Werte:<br>▪ License<br>▪ Admin Login/Logout<br>▪ Policy Saved<br>▪ Policy Published<br>▪ Policy Deleted<br>▪ Suspension Password Generated<br>▪ Global Policy Settings Changed<br>▪ Administration Changed<br>▪ Backup Succeeded<br>▪ Backup Failed<br>▪ Datenbank-Notlöschen<br>▪ Schlüssel für Zurücksetzen der Festplattenverschlüsselung gewährt<br>▪ Einmal-Schlüssel für Festplattenverschlüsselung gewährt<br>▪ Schlüssel für Wiederherstellung der Festplattenverschlüsselung gewährt |
| **Details** | Zeigt ggf. weitere Details an, wie etwa Lizenzalarmdetails, oder den Namen einer Richtlinie bei einem Policy-Veröffentlichungsereignis etc. |

## 5.10 Anzeigen von Shadow-Dateien

Das Datei-Shadowing bietet die Möglichkeit der Rückverfolgung und Erfassung von Kopien von Dateien, die zu/von externen Speichergeräten verschoben wurden. Dadurch erhalten Sie die einmalige Gelegenheit, nicht nur Informationen über die verschobenen Dateien, sondern auch über die Dateien selbst zu erhalten, wie nachfolgend beschrieben.

Wenn SafeGuard PortProtector dafür definiert ist, mit rollenbasierten Berechtigungen zu arbeiten, können nur Administratoren mit der Rollenberechtigung **Shadow-Dateien anzeigen** (siehe *Rollenbasiert (erweitert)*).

**So zeigen Sie die Shadow-Dateien an:**

1 Klicken Sie auf die Registerkarte **Logs**.

2 Klicken Sie auf die Registerkarte **Datei-Logs**. Bei Shadow-Dateien steht ein Kontrollhäkchen in der Spalte **Shadow-Dateien** und eine sequentielle, eindeutige ID in der Spalte **ID der Shadow-Datei** (siehe *Log-Tabelle*).

3 Wählen Sie die relevanten Organisationseinheiten aus (siehe *Filtern der Log-Tabelle nach Organisationseinheit*).

4 Definieren Sie eine neue File-Log-Abfrage (siehe *efinieren einer neuen Datei-Log-Abfrage*). Vergewissern Sie sich, dass Sie alle Optionen auf der Registerkarte **Shadowing** ausgefüllt haben (siehe *Shadowing-Eigenschaften – Datei-Logs*).

5 Klicken Sie auf **Ausführen**, um die Abfrage ausführen.

6 Öffnen Sie das entsprechende Fenster der Logdatensatz-Eigenschaften.

7 Wählen Sie **Öffnen** oder **Speichern** in der Spalte Shadow-Datei, um die Shadow-Datei aus dem Speicher herunterzuladen.

## 5.11 Logs von einem Standalone SafeGuard PortProtector Client-Computer lesen

Sie haben die Möglichkeit, Logs von einem Standalone SafeGuard PortProtector Computer zu lesen.

Wenn diese Sicherheitspolicy auf einen Standalone-Computer übernommen wird, konfigurieren Sie den Client so, dass er die lokalen Logs speichert statt sie über das Netz an den Management Server zu senden. Dadurch wird verhindert, dass der Agent regelmäßig versucht, Logs an den nicht verfügbaren Management Server zu senden.

**So konfigurieren Sie eine Policy für die lokale Log-Speicherung:**

1 Wählen Sie auf der Registerkarte *Policy* unter Einstellungen (linker Fensterausschnitt) die Option **Protokollierung**.

2 Wählen Sie bei *Logspeicher* die Option **Policy-spezifische Einstellungen festlegen:** und wählen Sie **Logs lokal speichern**.

**So lesen Sie Logs von einem Standalone-Client:**

1 Führen Sie auf dem Client-Computer den folgenden Befehl aus, der sicherstellt, dass die derzeit vom SafeGuard PortProtector Client genutzten Logs freigegeben und aus dem Computer kopiert werden können:
```
sc control sophosps 222
```

2 Verwenden Sie den folgenden Befehl, um die Log-Dateien (*.slg) aus ihrem standardmäßigen Speicherort (%programfiles%\sophos\SafeGuard PortProtector client\logs) zu kopieren:
```
xcopy "[Pfad zu Log-Dateien]" "[Zielpfad für Log-Datei ]" /c
/i /Y
```

3 Übertragen Sie die Log-Datei mittels eines Massenspeichergeräts oder eines anderen Übertragungsverfahrens vom Standalone-Client-Computer.

**Hinweis:** Dieser Vorgang lässt sich leicht automatisieren. Wenden Sie sich an den Sophos Support, um ein Tool zur Übertragung der Logs von Standalone-Endpunkten zu erhalten.

**So importieren Sie die Logs auf den Management Server:**

1. Kopieren Sie die Logs auf einen Computer, auf dem die SafeGuard PortProtector Management Console läuft.
2. Wählen Sie auf der Registerkarte Logs **Datei**>**Manueller Log-Import**. Das Dialogfeld *Log-Datei importieren* wird angezeigt.
3. Wählen Sie **Logs aus Ordner importieren**. Klicken Sie auf **Importieren**.
4. Wählen Sie bei *Ordner suchen* den Ordner, der die Logs enthält, und klicken Sie auf **OK**.

Die Logs erscheinen jetzt auf der Registerkarte Logs.

# 6 Verwalten von Clients

## Über dieses Kapitel

Dieses Kapitel beschreibt die Clients-Welt, die als Zentralstelle für das Ausführen von Operationen auf den SafeGuard PortProtector Clients in der Organisation dient. Dieses Kapitel enthält die folgenden Abschnitte:

- *Übersicht* liefert eine kurze Beschreibung der Clients-Welt.
- *Kurze Übersicht über die Clients-Welt* beschreibt das Hauptfenster der Clients-Welt.
- *Clients-Tabelle* beschreibt die in der Clients-Tabelle verfügbaren Information, und wie die Tabelle verwaltet wird.
- *Fensterausschnitt Client-Eigenschaften* beschreibt die Informationen und Links im Fensterausschnitt Client-Eigenschaften.
- *Filtern von Clients* beschreibt die Struktur und deren Nutzung zur Anzeige der gewünschten Clients.
- *Exportieren der Clients-Tabelle* beschreibt das Exportieren der Clients-Tabelle als XML-Datei, die von MS Excel für Auswertungszwecke genutzt werden kann.
- *Vorbereiten des Client-Deployments* liefert Informationen darüber, was vor dem Deployment von SafeGuard PortProtector Clients auf Endpunkten zu tun ist.
- *Aktualisieren einer Policy auf einem Client* beschreibt, wie eine Policy auf einem Client aktualisiert wird.
- *Abrufen der aktuellsten Informationen von einem Client* beschreibt, wie Logs erfasst werden, um die aktuellsten verfügbaren Informationen von Clients zu sehen.
- *Verfolgen des Fortschritt von Client-Tasks* beschreibt, wie der Fortschritt von Client-Tasks, wie etwa Policy-Aktualisierung oder Logerfassung, verfolgt werden.
- *Vorübergehendes Aufheben des SafeGuard PortProtector Schutzes* beschreibt das Generieren eines Kennworts, das die temporäre Suspendierung eines Clients ermöglicht.
- *Zurücksetzen und Aktualisieren des Client-Status* beschreibt, wie Client aus der Clients-Tabelle entfernt werden, die nicht geschützt werden.
- *Löschen von nicht in der Domäne befindlichen* Clients beschreibt, wie Clients gelöscht werden, die nicht in der Domäne sind.
- *Auditing von Geräten* beschreibt, wie SafeGuard PortAuditor von der Management Console aus gestartet wird

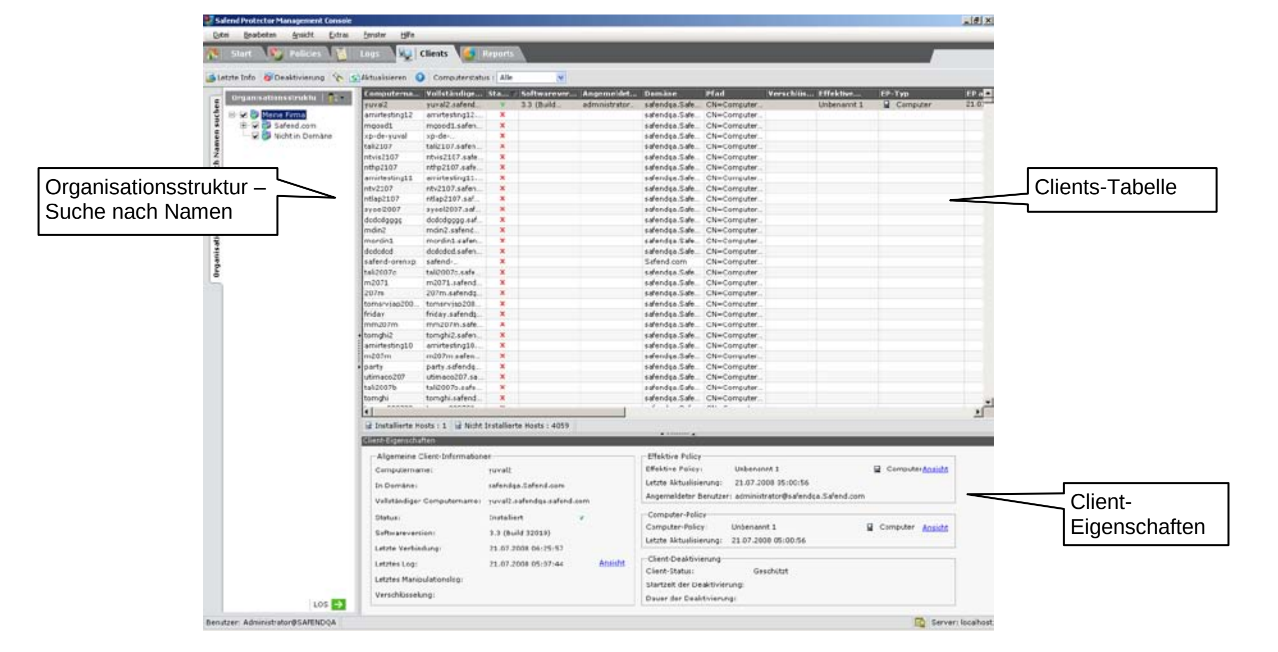
## 6.1 Übersicht

Die Clients-Welt dient als zentrale Stelle zur Anzeige des Status und der Details von SafeGuard PortProtector Clients, zur Ausführung von Tasks wie etwa das Aktualisieren von Policies auf den Clients und Erfassen von Logs von den Clients, zum Anzeigen des Taskverlaufs, zum Generieren eines Kennworts für die temporäre Aufhebung des Schutzes auf einem SafeGuard PortProtector Client etc.

## 6.2 Kurze Übersicht über die Clients-Welt

**So öffnen Sie die Clients-Welt:**

Klicken Sie auf die Registerkarte **Clients**. Das Fenster *Clients* wird angezeigt:



### 6.2.1 Menü Datei

Über das Menü *Datei* in der Clients-Welt können Sie neue Welt-Fenster öffnen, die Clients-Tabelle exportieren, sich von der Management Console abmelden und die Anwendung beenden.




Das Menü *Datei* enthält folgende Optionen:

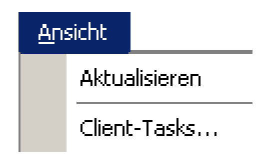
| Option | Beschreibung |
| --- | --- |
| **Neu** | Öffnet ein Untermenü, über das Sie ein neues Policy-, ein neues Client Log-, ein neues Server Log- oder ein neues File Log-Fenster öffnen können. |
| **Benutzerrolle ändern** | Einem SafeGuard PortProtector-Administrator können mehrere Rollen zugewiesen werden, um die verschiedenen Domänenpartitionen zu definieren, für die er verantwortlich ist. Nachdem sich ein solcher Administrator angemeldet hat, wird automatisch ein Auswahlfenster angezeigt, in dem er die entsprechende Rolle für seine Arbeit auswählen kann.<br><br>**Hinweis:** Eine Benutzerrolle definiert die Funktionen, Organisationseinheiten und Domänen einer Organisation, auf die ein SafeGuard PortProtector-Administrator zugreifen kann, wie in *Definieren von Rollen* beschrieben.<br><br>Über die Option **Benutzerrolle ändern** kann ein solcher Administrator von dieser Rolle jederzeit zu einer anderen, ihm zugewiesenen Rolle wechseln. |
| **Exportieren** | Exportiert die Clients-Tabelle in eine externe Datei. |
| **Abmelden** | Meldet den aktuellen Benutzer von der Management Console ab. |
| **Beenden** | Meldet den aktuellen Benutzer ab und schließt die SafeGuard PortProtector Management Console. |

### 6.2.2 Menü Bearbeiten

In der Clients-Welt sind die Optionen in diesem Menü deaktiviert.

### 6.2.3 Menü Ansicht

Über das Menü *Ansicht* können Sie das aktuelle Fenster aktualisieren und den Fortschritt von Client-Tasks anzeigen lassen.




Das Menü *Ansicht* enthält folgende Optionen:

| Option | Beschreibung |
| --- | --- |
| **Refresh** | Aktualisiert die Clients-Tabelle entsprechend der Auswahl in der Organisationsstruktur und aktualisiert die Datensätze der Clients-Tabelle gemäß den aktuellen Logs. |
| **Client Tasks** | Zeigt den Verlauf der Client-Tasks (weitere Informationen finden Sie in *Verfolgen des Fortschritts von* Client-Tasks). |

### 6.2.4 Menü Extras

Das Menü *Extras*, das bei allen Welten gleich ist, ist im Kapitel *Erste Schritte*, beschrieben.

### 6.2.5 Menü Fenster

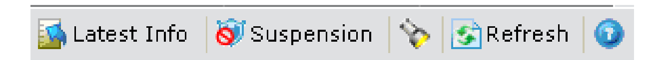
Das Menü Fenster, das bei allen Welten gleich ist, ist im Kapitel *Erste Schritte*, beschrieben.

### 6.2.6 Menü Hilfe

Das Menü *Hilfe*, das bei allen Welten gleich ist, ist im Kapitel *Erste Schritte*, beschrieben.

### 6.2.7 Symbolleiste

Die Symbolleiste der Clients-Welt bietet schnellen Zugriff auf häufig genutzte Funktionen. Sie wird unterhalb der Menüleiste angezeigt und enthält die folgenden Schaltflächen:




Nachfolgend eine kurze Beschreibung der einzelnen Schaltflächen in der Symbolleiste:

| Schaltfläche | Beschreibung |
|---|---|
| **Letzte Info abrufen** | Ruft die durch das Erfassen der Logs die aktuellsten Informationen von den einzelnen Clients ab (weitere Informationen hierzu finden Sie in *Abrufen der aktuellsten Informationen von einem* Client). |
| **Suspendierungskennwort gewähren** | Gewährt ein Suspendierungskennwort zu, mit dem der Schutz eines Clients temporär aufgehoben werden kann. |
| **Geräte-Audit** | Startet SafeGuard PortAuditor (siehe *Auditing von Geräten*). |
| **Aktualisieren** | Aktualisiert die Clients-Tabelle entsprechend der Auswahl in der Organisationsstruktur und aktualisiert die Datensätze der Clients-Tabelle gemäß den aktuellen Logs. |
| **Hilfe** | Zeigt die Kontexthilfe des aktiven Fensters und ermöglicht den Zugriff auf andere Hilfethemen. |

### 6.2.8 Arbeitsbereich

Der Arbeitsbereich der Clients-Welt ist in zwei Bereiche unterteilt:

- **Clients-Tabelle** – Diese Tabelle erscheint im oberen rechten Fensterausschnitt und zeigt eine Tabelle der Clients im ausgewählten Element der Organisationsstruktur. Bevor Sie eine Auswahl auf den Registerkarten **Organisationsstruktur** oder **Suche nach Namen** (unten beschrieben) getroffen haben, ist dieser Bereich leer. Weitere Informationen finden Sie in *Clients-Tabelle*.
- **Organisationsstruktur** und **Nach Namen suchen** – Diese Registerkarten erscheinen im linken Fensterausschnitt. Diese Registerkarten dienen als Filter für die in der Clients-Tabelle anzuzeigenden Datensätze. Die Registerkarten werden in *Filtern von Clients* behandelt.
- **Client-Eigenschaften** – Dieser Fensterausschnitt wird unter der Clients-Tabelle angezeigt und enthält die Eigenschaften des in der Clients-Tabelle ausgewählten Computers. Weitere Informationen finden Sie in *Fensterausschnitt Client-Eigenschaften*.

## 6.3 Clients-Tabelle

Die Clients-Tabelle zeigt Informationen zu den Clients, die die in der Organisationsstruktur ausgewählten Elemente der Organisation schützen.

Die Clients-Tabelle zeigt folgende Spalten:

| Spalte | Beschreibung |
|---|---|
| **Computername** | Der Name des Computers, auf den sich die Spalten in der Zeile beziehen. |
| **Vollständiger Computername** | Der vollständige Name des Computers, auf den sich die Spalten in der Zeile beziehen, einschließlich seiner Domänenendung. |
| **Status** | **Served** ( ) – durch SafeGuard PortProtector geschützter Client, oder **Not Served** ( ) – nicht geschützt. |
| **Software Version** | Die auf dem Computer installierte Version von SafeGuard PortProtector. |
| **Angemeldeter Benutzer** | Wenn ein Benutzer angemeldet ist, erscheinen hier sein Benutzer- und Domänenname. |
| **Domäne** | Der Domänenname. |
| **Pfad** | Der Pfad zum Client-Standort in Active Directory/Novell eDirectory. |
| **Effective Policy (EP)** | Der Name der Policy, die auf dem Computer in Kraft ist. Wenn auf diesem Client Policies zusammengeführt sind, werden alle zusammengeführten Policies aufgeführt. |
| **EP-Type** | Der Typ der geltenden Policy – **Computer** ( ) oder **Benutzer** ( ). |
| **EP aktualisiert** | Datum und Uhrzeit, wann die geltende Policy zuletzt aktualisiert wurde. |

| Spalte | Beschreibung |
|---|---|
| **Computer Policy (CP)** | Der Name der Computer-Policy. Dies kann von Effektive Policy abweichen, wenn eine Benutzer-Policy in Kraft ist. |
| **CP Updated** | Datum und Uhrzeit, wann die Computer-Policy zuletzt aktualisiert wurde. |
| **Last Handshake** | Datum und Uhrzeit des letzten Handshakes zwischen dem Client und dem Management Server. |
| **Received Logs** | Datum und Uhrzeit, wann zuletzt Logs empfangen wurden. |
| **Received Tampering Logs** | Datum und Uhrzeit, wann zuletzt Manipulationslogs empfangen wurden. |
| **Suspension Status** | **Suspended –** Schutz ist aufgehoben, ansonsten **Protected**. |
| **Suspension Start Time** | Datum und Uhrzeit, wann die Suspendierung begann. |
| **Suspension Duration** | Der vom Administrator definierte Zeitraum, für den dieser Computer suspendiert sein wird. |

Sie können die Tabellenansicht folgendermaßen ändern:

- **Sortieren** Sie die Tabelle, indem Sie auf den Spaltentitel der Spalte klicken, nach der Sie sortieren möchten. Klicken Sie nochmals auf die Überschrift, um zwischen auf- und absteigender Reihenfolge zu wechseln. Sie können eine zweite Sortierebene hinzufügen, indem Sie die **Umschalttaste** drücken und auf den zweiten Spaltentitel klicken.
- **Ändern Sie die Spaltenbreite**, indem Sie die Spaltentrennlinien an die gewünschte Stelle ziehen.
- **Verschieben Sie eine Spalte**, indem Sie sie an die gewünschte Position ziehen.

## 6.4 Fensterausschnitt Client-Eigenschaften

Der Fensterausschnitt Client-Eigenschaften wird unter der Clients-Tabelle angezeigt und enthält die Eigenschaften des in der Clients-Tabelle ausgewählten Clients. Die Details in diesem Fensterausschnitt sind mit denen in der Tabelle identisch. In diesem Fensterausschnitt werden Informationen bezüglich des ausgewählten Tabellendatensatzes angezeigt, die in den folgenden Abschnitten angeordnet sind:

- **Allgemeine Client-Informationen:** Zeigt allgemeine Information zum Computer und zum Client und enthält eine Angabe darüber, ob der Client geschützt (Served) ist, sowie Links zur Anzeige von Logs und Manipulationslogs für den Client. Ein Gefahrensymbol wird angezeigt, wenn der Computer mindestens ein Mal manipuliert wurde. Angezeigt wird auch, ob die interne Festplatte verschlüsselt ist oder nicht, sowie das genaue Datum und die genaue Zeit, wann die ursprüngliche Verschlüsselung abgeschlossen wurde.
- **Effektive Policy:** Zeigt Informationen zur derzeit geltenden Policy (die geltende Policy ist eine andere als die Computer-Policy, wenn ein Benutzer mit einer Benutzer-Policy angemeldet ist). Enthält einen Link zur Anzeige der aktuell geltenden Policy.
- **Computer-Policy:** Zeigt Informationen zur Computer-Policy (die Computer-Policy ist u.U. nicht die geltende Policy, wenn ein Benutzer mit einer Benutzer-Policy angemeldet ist). Enthält einen Link zur Anzeige der Computer-Policy.
- **Client-Deaktivierung**: Zeigt Informationen bezüglich der Client-Suspendierung. Ein Gefahrensymbol wird angezeigt, wenn der Computer derzeit suspendiert ist.

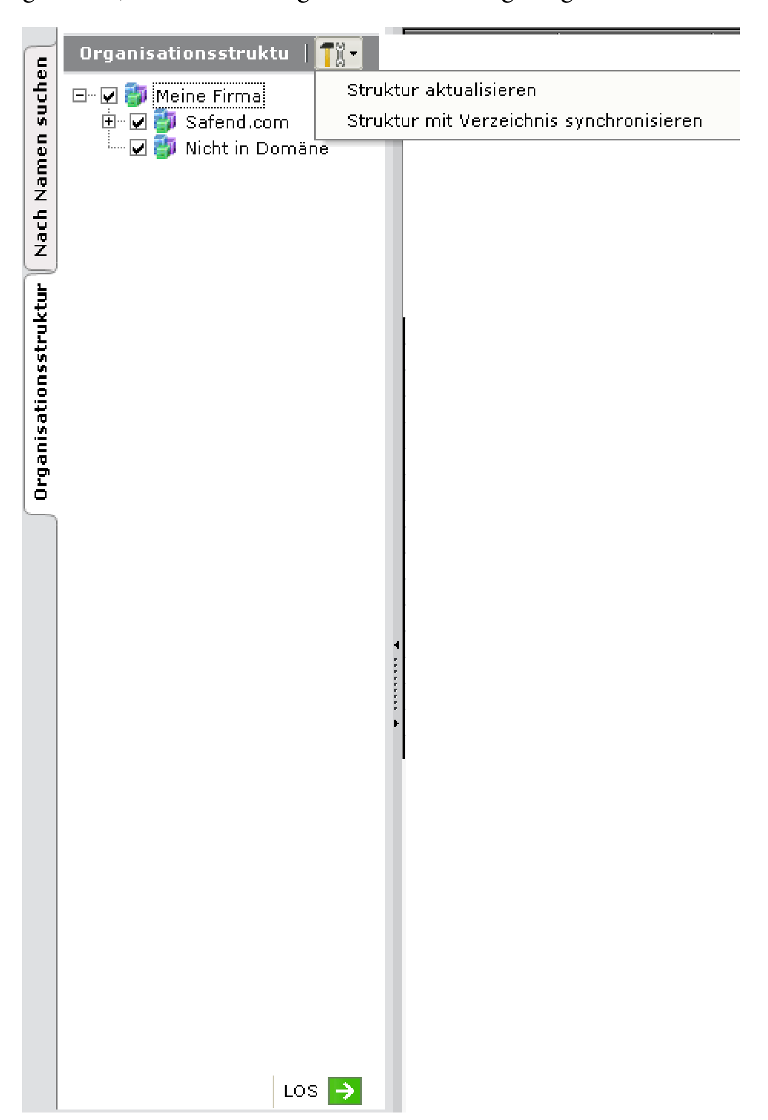
## 6.5 Filtern von Clients

Die linke Seite des Clients-Fensters enthält zwei Registerkarten, die Ihnen dabei helfen die Computer zu bestimmen, deren Logs in der Clients-Tabelle angezeigt werden sollen.

### 6.5.1 Filtern der Clients-Tabelle nach Organisationseinheit

Die *Organisationsstruktur* ist ein Tool, mit dem Sie die Organisationseinheiten bestimmen können, deren Clients in der Clients-Tabelle angezeigt werden sollen. Dieser Abschnitt beschreibt, wie die Organisationsstruktur gehandhabt und aus der Struktur heraus festgelegt wird, welche Clients in der Clients-Tabelle angezeigt werden.

Die Registerkarte *Organisationsstruktur* zeigt die Domäne(n), Organisationseinheiten sowie die Gruppe Nicht in Domäne (die alle Computer enthält, die derzeit nicht zu der Domäne gehören), wie in der folgenden Abbildung dargestellt:




**Hinweis:** Die Organisationsstruktur ist nur anwendbar, wenn Sie Active Directory/Novell eDirectory einsetzen. Andernfalls wird nur eine Gruppe in der Struktur angezeigt – Nicht in Domäne. Durch Auswahl dieser Gruppe werden alle Computer ausgewählt.

**So wählen Sie die gewünschten Organisationseinheiten aus:**

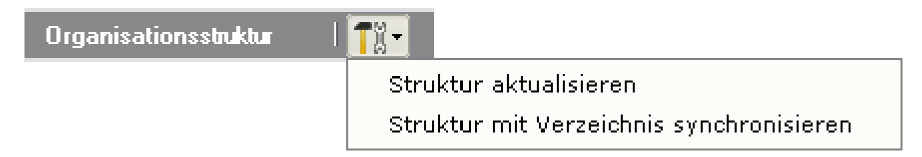
1 Erweitern Sie bei Bedarf die Organisationsstruktur, so dass Organisationseinheiten auf niedrigeren Ebenen angezeigt werden.

2 Wählen Sie die gewünschte Domäne oder Organisationseinheiten durch Aktivieren der entsprechenden Kontrollkästchen aus.

3 Klicken Sie unten auf der Registerkarte *Organisationsstruktur* auf **LOS** ( ). Die Informationen, die jetzt in der Clients-Tabelle angezeigt werden, stammen ausschließlich von Clients, die zu dem in der Struktur gewählten Element gehören.

### 6.5.1.1 Aktualisieren der Organisationsstruktur

Bevor Sie Ihre Auswahl in der Struktur treffen, möchten Sie sie vielleicht aktualisieren. Sie können die Struktur entweder im SafeGuard PortProtector Management Server aktualisieren oder sie mit Active Directory/Novell eDirectory synchronisieren (das Directory kann aktueller sein, aber es kann auch länger dauern). Die Struktur wird über das Menü *Organisationsstruktur* (unten dargestellt) aktualisiert, das sich oben in der Registerkarte *Organisationsstruktur* befindet.




**So aktualisieren Sie die Organisationsstruktur im Management Server:**

Klicken Sie im Menü *Organisationsstruktur* auf **Struktur aktualisieren**. Die Struktur wird aktualisiert.

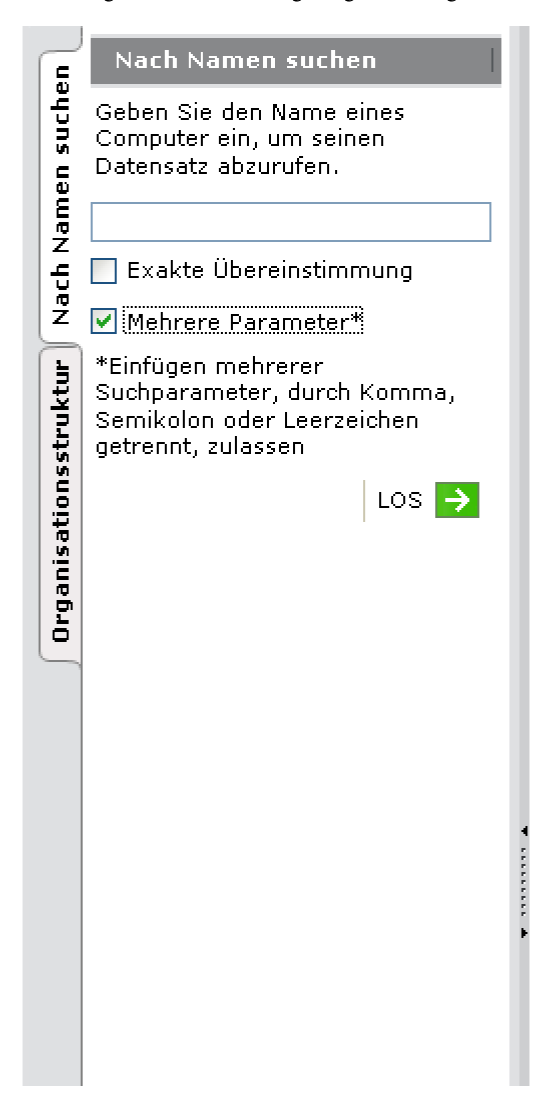
**So aktualisieren Sie die Organisationsstruktur im Directory:**

Klicken Sie im Menü *Organisationsstruktur* (siehe vorherige Abbildung) auf **Struktur mit Verzeichnis synchronisieren**. Die Struktur wird aktualisiert, aber dieser Vorgang kann eine Weile dauern.

## 6.5.2 Filtern nach Namen

Die Registerkarte *Nach Namen suchen* ist ein weiteres Werkzeug, mit dem Sie die Computer bestimmen können, deren Datensätze in der Clients-Tabelle angezeigt werden. Dieser Abschnitt beschreibt, wie diese Registerkarte zur Festlegung der in der Clients-Tabelle anzuzeigenden Clients verwendet wird.

Die folgende Abbildung zeigt die Registerkarte *Nach Namen Suchen*:



**So suchen Sie nach bestimmten Computern:**

1 Geben Sie im Textfeld den Namen des anzuzeigenden Computers oder Benutzers ein, dessen Datensatz in der Tabelle angezeigt werden soll. Sie können mehrere Namen durch Komma, Semikolon oder Leerzeichen getrennt eingeben.

2 Markieren Sie das Kontrollkästchen **Exakte Übereinstimmung**, wenn Sie in der Tabelle Datensätze für einen Computer mit einem Namen anzeigen möchten, der genau mit der von Ihnen im Textfeld eingegebenen Zeichenfolge übereinstimmt. In diesem Fall müssen Sie den vollständigen Computernamen eingeben (einschließlich der Domänenendung). Wenn **Exakte Übereinstimmung** nicht markiert ist, werden in der Clients-Tabelle Datensätze für alle Computer angezeigt, deren Name die von Ihnen eingegebene Zeichenfolge enthält.

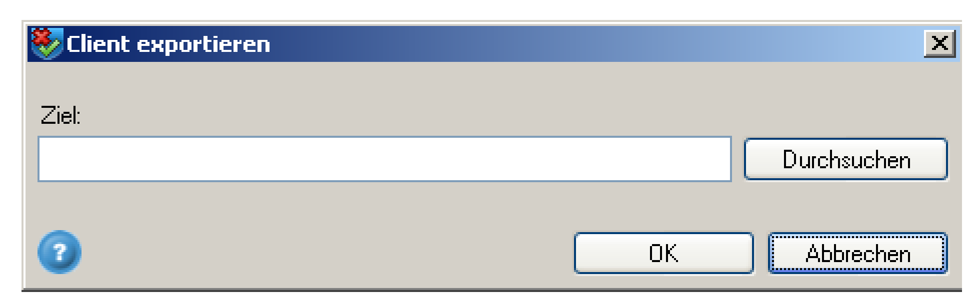
3 Klicken Sie unter dem Textfeld auf **LOS** (). Die jetzt in der Tabelle angezeigten Client-Datensätze beziehen sich auf die Computer, deren Name Ihren Suchkriterien entspricht. Wenn kein Computer gefunden wird, dessen Name Ihren Suchkriterien entspricht, ist die Tabelle leer.

## 6.6 Exportieren der Clients-Tabelle

Wenn Sie die Clients-Tabelle in eine externe Datei exportieren möchten, um sie zu drucken oder weitere Analysen durchzuführen, ist dies über das Fenster *Clients exportieren* möglich.

**So öffnen Sie das Fenster *Clients exportieren*:**

Wählen Sie im Menü *Datei* die Option **Exportieren**. Das Fenster *Clients exportieren* wird angezeigt.




### 6.6.1 Exportieren der Clients-Tabelle in eine externe Datei

Verwenden Sie diese Option, um die Clients-Tabelle zu exportieren, um sie zu drucken oder weitere Analysen durchzuführen. Die exportierte Datei wird im XML-Format gespeichert, das ganz einfach z. B. mit MS Excel geöffnet werden kann.

**So exportieren Sie Clients:**

1 Klicken Sie auf die Schaltfläche **Durchsuchen**, um einen Pfad auszuwählen (und einen Dateinamen einzugeben) oder den Pfad für die exportierte Datei einzugeben.

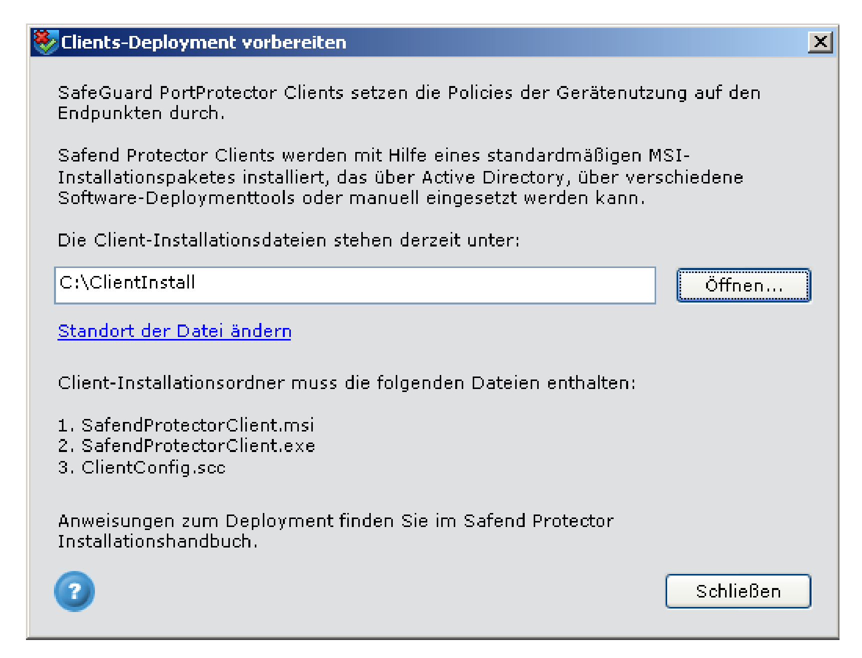
2 Klicken Sie auf **OK**. Ein Verlaufsfenster wird angezeigt, und der Export beginnt.

## 6.7 Vorbereiten des Client-Deployments

Das Deployment von SafeGuard PortProtector Client (Installation) erfolgt über ein standardmäßiges MSI-Installationspaket. Die Installation kann über Active Directory, über verschiedene andere Deployment-Tools oder manuell erfolgen. Vor dem Deployment können Sie überprüfen, ob die erforderlichen Dateien vorhanden sind.

**So bereiten Sie die Client-Installation vor:**

Klicken Sie im Menü *Extras* auf **Client-Deployment vorbereiten**. Das Fenster *Clients-Deployment vorbereiten* wird angezeigt:




### 6.7.1 Clients-Deployment vorbereiten

Dieses Fenster zeigt den aktuellen Speicherort der SafeGuard PortProtector Client-Installationsdateien. Der Speicherort der Client-Installationsdateien wird auf der Registerkarte Clients im Fenster Administration definiert (siehe Kapitel *Administration*).

Der Client-Installationsordner muss die folgenden Dateien enthalten:

- SafeGuardPortProtectorClient.msi
- SafeGuardPortProtectorClient.exe
- ClientConfig.scc

Eine detaillierte Erläuterung der Client-Installation finden Sie im *SafeGuard PortProtector Installationshandbuch*.

**So bereiten Sie das Client-Deployment vor:**

Klicken Sie im Fenster auf **Öffnen**, und prüfen Sie, ob die erforderlichen Dateien im Installationsordner vorhanden sind. Falls nicht, können Sie zum Fenster *Administration* wechseln, indem Sie auf den Link **Standort der Datei ändern** klicken.

Eine vollständige Anleitung für das Deployment von SafeGuard PortProtector Clients finden Sie im *SafeGuard PortProtector Installationshandbuch*.

## 6.8 Aktualisieren einer Policy auf einem Client

**Hinweis:** Da SafeGuard PortProtector für diese Option WMI nutzt, können Sie diese Aktion nur dann ausführen, wenn ein Windows-Benutzer mit lokalen Administratorrechten auf den Ziel-Endpunkten definiert ist, vorausgesetzt Sie habe im Fenster *Administration* Novell als Ihr Verzeichnis gewählt.

Wie in *Kapitel 4, Verteilen von Policies*, erläutert, werden Policies auf dem SafeGuard PortProtector Client dadurch aktualisiert, dass der Client den GPO-Dienst oder die Registry-Datei in vordefinierten Intervallen prüft und die Policy aktualisiert, falls sie geändert wurde. Wenn Sie kürzlich eine Policy für eine bestimmte Organisationseinheit oder einen bestimmten Computer bearbeitet haben, möchten Sie vielleicht die betroffenen SafeGuard PortProtector Clients auffordern, bei der nächsten Gelegenheit nach einer aktualisierten Policy zu suchen.

Es gibt. zwei Möglichkeiten für das Aktualisieren von Policies:

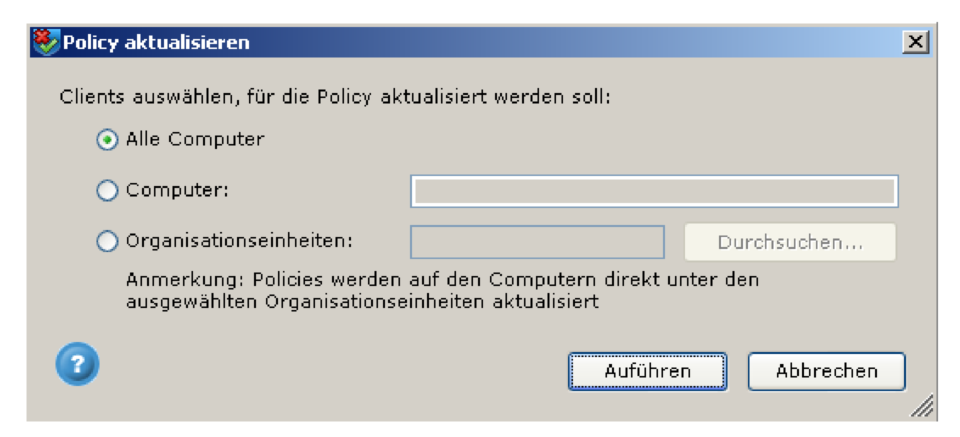
- **Über das Menü *Extras*:** Mit dieser Option können Sie Policies für jede beliebige Organisationseinheit bzw. jeden beliebigen Computer aktualisieren.
- **Durch Klicken mit der rechten Maustaste:** Mit dieser Option können Sie Policies auf zuvor ausgewählten Clients durch Klicken mit der rechten Maustaste auf Organisationseinheiten in der Organisationsstruktur oder durch Klicken mit der rechten Maustaste auf geschützte Clients in die Clients-Tabelle aktualisieren.

### 6.8.1 Aktualisieren einer Policy auf einem beliebigem Client

Das Aktualisieren einer Policy wird im Fenster *Policy aktualisieren* aktiviert.

**So öffnen Sie das Fenster *Policy aktualisieren*:**

Wählen Sie im Menü *Extras* die Option **Policy aktualisieren.** Das Fenster *Policy aktualisieren* wird angezeigt:



#### 6.8.1.1 Aktualisieren einer Client-Policy

Wenn Sie kürzlich eine Policy für eine bestimmte Organisationseinheit oder einen bestimmten Computer bearbeitet haben, möchten Sie vielleicht die betroffenen SafeGuard PortProtector Clients auffordern, bei der nächsten Gelegenheit nach einer aktualisierten Policy zu suchen.

**So aktualisieren Sie eine Policy:**

1 Markieren Sie die gewünschte Optionsschaltfläche wie folgt:

- **Alle Computer**: Klicken Sie auf diese Option, wenn Sie Policies auf allen Computer in der Organisation aktualisieren möchten.
- **Organisationseinheiten**: Klicken Sie auf diese Option, wenn Sie Policies für eine oder mehrere Organisationseinheiten aktualisieren möchten. Klicken Sie auf **Durchsuchen**, und wählen Sie die gewünschten Organisationseinheiten in der Organisationsstruktur. Die ausgewählten Einheiten werden im Feld **Organisationseinheiten** angezeigt.
- **Computer**: Klicken Sie auf diese Option, wenn Sie eine Policy für einen oder mehrere Computer aktualisieren möchten, und geben Sie den Computernamen in dem Feld ein. Wenn Sie mehrere Computernamen eingeben möchten, trennen Sie sie mit einem Doppelpunkt oder Semikolon ab.

2 Klicken Sie auf **Ausführen**. An die ausgewählten Computer wird eine Benachrichtigung gesendet, nach einer neuen Policy zu suchen, und das Fenster *Client-Task Fortschritt* wird angezeigt. Sie können den Verlauf des Aktualisierungsvorgangs in diesem Fenster verfolgen, wie in *Verfolgen des Fortschritts von Client-Tasks* erläutert.

### 6.8.2 Aktualisieren einer Policy auf zuvor ausgewählten Clients

Diese Option führt dieselben Aktionen aus, wie im vorangehenden Abschnitt beschrieben. Sie ermöglicht es Ihnen aber auch, die Clients für die Aktualisierung vorher auszuwählen.

**So aktualisieren Sie Policies (durch Klicken mit der rechten Maustaste):**

1 Wählen Sie in der Organisationsstruktur die gewünschten Elemente aus, oder wählen Sie die gewünschten Computer in der Tabelle aus.

2 Klicken Sie mit der rechten Maustaste. Wählen Sie in dem dann angezeigten Menü die Option **Policy aktualisieren**. An die ausgewählten Computer wird eine Benachrichtigung gesendet, nach einer neuen Policy zu suchen, und das Fenster *Client-Task Fortschritt* wird angezeigt. Sie können den Verlauf des Aktualisierungsvorgangs in diesem Fenster verfolgen (siehe auch *Verfolgen des Fortschritts von Client-Tasks*).

## 6.9 Abrufen der aktuellsten Informationen von einem Client

**Hinweis:** Da SafeGuard PortProtector für diese Option WMI nutzt, können Sie diese Aktion nur dann ausführen, wenn ein Windows-Benutzer mit lokalen Administratorrechten auf den Ziel-Endpunkten definiert ist, vorausgesetzt Sie habe im Fenster *Administration* Novell als Ihr Verzeichnis gewählt.

Unter Umständen möchten Sie Client-Informationen so zeitnah wie möglich einsehen. Mit dieser Option können Sie Logs erfassen und die aktuellsten Informationen von geschützten Computern außerhalb der vordefinierten Erfassungszeiten anzeigen. Bei Aktivierung dieser Funktion werden alle Logtypen erfasst.

Es gibt zwei Wege für die Erfassung von Logs:

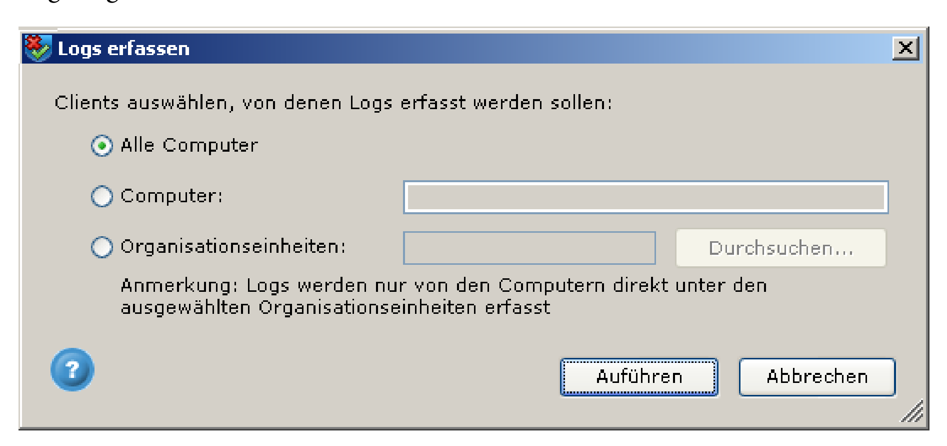
- **Über das Menü *Extras* oder über die Symbolleiste:** Mit dieser Option können Sie Logs für jede beliebige Organisationseinheit bzw. jeden beliebigen Computer erfassen.
- **Durch Klicken mit der rechten Maustaste:** Mit dieser Option können Sie Logs von zuvor ausgewählten Clients durch Klicken mit der rechten Maustaste auf Organisationseinheiten in der Organisationsstruktur oder durch Klicken mit der rechten Maustaste auf geschützte Clients in die Clients-Tabelle erfassen.

### 6.9.1 Erfassen von Logs von einem beliebigen Client

Die Logerfassung wird im Fenster *Logs erfassen* aktiviert.

**So öffnen Sie das Fenster *Logs erfassen*:**

Wählen Sie im Menü *Extras* die Option **Retrieve Latest Info** (**collect logs**), oder klicken Sie in der Symbolleiste auf die Schaltfläche **Retrieve Latest Info**. Das Fenster *Logs erfassen* wird angezeigt:



#### 6.9.1.1 Erfassen von Logs

Mit dieser Option können Sie Logs erfassen und die aktuellsten Informationen von geschützten Computern außerhalb der vordefinierten Erfassungszeiten anzeigen. Bei Aktivierung dieser Funktion werden alle Logtypen erfasst.

**So erfassen Sie Logs:**

1 Klicken Sie auf die Optionsschaltfläche für die gewünschte Option:

- **Alle Computer**: Markieren Sie diese Option, wenn Sie Logs von allen Computer in der Organisation erfassen möchten.
- **Organisationseinheiten**: Markieren Sie diese Option, wenn Sie Logs von einer oder mehreren Organisationseinheiten erfassen möchten. Klicken Sie auf **Durchsuchen**, und wählen Sie die gewünschten Organisationseinheiten aus der Firmenstruktur. Die ausgewählten Einheiten werden im Feld **Organisationseinheiten** angezeigt.
- **Computer**: Klicken Sie auf diese Option, wenn Sie Logs von einem oder mehreren Computern erfassen möchten, und geben Sie den Computernamen in dem Feld ein. Wenn Sie mehrere Computernamen eingeben möchten, trennen Sie sie mit einem Doppelpunkt oder Semikolon ab.

2 Klicken Sie auf **Ausführen**. Die Erfassung der Logs von den ausgewählten Computern beginnt, und das Fenster *Verlauf der Client Tasks* wird angezeigt. Sie können den Verlauf des Aktualisierungsvorgangs in diesem Fenster verfolgen (siehe auch *Verfolgen des Fortschritts von Client-Tasks*).

### 6.9.2 Erfassen von Logs von zuvor ausgewählten Clients

Diese Option führt dieselben Aktionen aus, wie im vorangehenden Abschnitt beschrieben. Sie ermöglicht es Ihnen aber, die Clients für die Logerfassung vorher auszuwählen.

**So erfassen Sie Logs (durch Klicken mit der rechten Maustaste):**

1 Wählen Sie in der Organisationsstruktur die gewünschten Knoten aus.

2 Klicken Sie mit der rechten Maustaste. Ein Menü wird angezeigt.

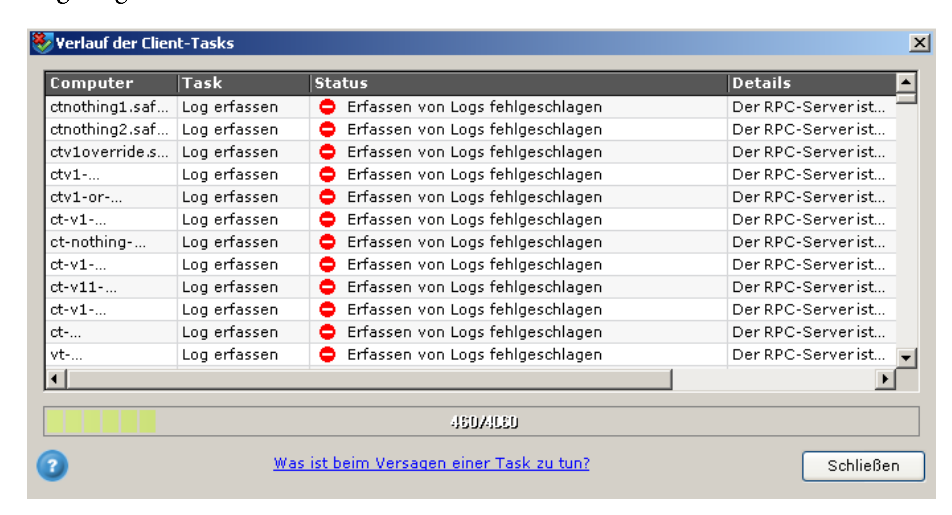
3 Wählen Sie im Menü die Option **Retrieve Latest Info**. Die Erfassung der Logs von den ausgewählten Computern beginnt, und das Fenster *Verlauf der Client-Tasks* wird angezeigt. Sie können den Verlauf des Aktualisierungsvorgangs in diesem Fenster verfolgen, wie in *Verfolgen des Fortschritts von Client-Tasks* erläutert.

## 6.10 Verfolgen des Fortschritts von Client-Tasks

Wenn die Anwendung Tasks ausführt (wie etwa das Erfassen von Logs oder das Aktualisieren von Policies), können Sie den Verlauf dieser Tasks im Fenster Client Tasks Progress *anzeigen lassen.*

**So verfolgen Sie den Fortschritt von Client-Tasks:**

Wählen Sie im Menü *Ansicht* die Option **Client-Tasks.** Das Fenster *Verlauf der Client-Tasks* wird angezeigt. In diesem Fenster können Sie den Verlauf der Tasks sehen.




### 6.10.1 Verlauf der Client-Tasks

Das Fenster *Verlauf der Client-Tasks* zeigt alle derzeit laufenden Tasks mit dem Status der jeweiligen Task und den jeweils auftretenden Statusänderungen. Für jeden Client wird eine Zeile angezeigt (es sei denn, dass für denselben Client eine Policy-Aktualisierung und eine Logerfassung gleichzeitig laufen, so dass zwei Zeilen für den betroffenen Client angezeigt werden). Für die wechselnden Phasen der Tasks werden auch die Werte in der Spalte *Status* geändert. Eine abgeschlossene Task hat den Status **Abgeschlossen** oder **Fehlgeschlagen**. Beim Status Fehlgeschlagen wird ein Grund angegeben.

Das Fenster *Verlauf der Client-Tasks*:

| Option | Beschreibung |
|---|---|
| **Computer** | Zeigt den vollständigen Computernamen an. |
| **Task** | Zeigt die Task an, die der Client ausführt (Log erfassen, Policy aktualisieren. |
| **Status** | Zeigt den aktuellen Status der Task (Abgeschlossen, Anstehend, Pushen der Policy, Fehlgeschlagen). |
| **Details** | Wenn der Status Fehlgeschlagen ist, wird der Grund angezeigt. |

**Hinweis:** Da SafeGuard PortProtector für die Ausführung von Remote-Client-Tasks WMI nutzt, müssen WMI-Ports geöffnet sein, damit der Befehl durchgeht. *Client-Task-Fehler* Weitere Informationen hierzu finden Sie in.

**Hinweis:** Wenn Sie im Fenster Administration Novell als Ihr Verzeichnis gewählt haben, können Sie diese Aktion nur ausführen, wenn ein Windows-Benutzer mit lokalen Administratorrechten auf den Ziel-Endpunkten definiert ist.

#### 6.10.1.1 Client-Task-Fehler

Da SafeGuard PortProtector für die Ausführung von Remote-Client-Tasks die WMI-Infrastruktur von Windows nutzt, müssen WMI-Ports geöffnet sein, damit der Befehl durchgeht. Es kann 3 verschiedene Fälle geben, bei denen der WMI-Befehl nicht richtig funktioniert. Wenn eine oder mehrere Client-Tasks fehlgeschlagen sind, prüfen Sie Folgendes anhand der in der Spalte **Details** im Fenster *Verlauf der Client Tasks* angezeigten Aufgabendetails:

| Aufgabendetails | Lösung |
|---|---|
| **Access Denied** | Vergewissern Sie sich, dass die definierten Server-Berechtigungen, die für den Scan herangezogen werden, lokale Administratorrechte auf dem Remote-Computer beinhalten. Weitere Informationen hierzu finden Sie in *Server-Berechtigungen*. |
| **The service cannot be started** | Vergewissern Sie sich, dass der WMI-Dienst auf dem Remote-Computer gestartet und auf automatischen Start eingestellt ist. |
| **The RPC server is unavailable** | Vergewissern Sie sich, dass die WMI-Ports bei der aktiven Firewall zugelassen sind, und dass "Remote Administration" in der Windows-Firewall zugelassen ist |

**So überprüfen Sie die WMI-Konnektivität in Ihrer Umgebung:**

1 Wählen Sie auf dem Server-Computer **Ausführen** im Menü *Start* und geben Sie **wmimgmt.msc** ein.

2 Klicken Sie auf der linken Seite mit der rechten Maustaste auf **WMI Control** (**Local**) und wählen Sie **Connect to another computer**.

3 Wählen Sie einen anderen **Computer** und geben Sie den Namen des Computers ein, mit dem Sie die Kommunikation herstellen möchten. Klicken Sie auf **OK**.

4 Klicken Sie auf der linken Seite mit der rechten Maustaste auf **WMI Control** [**hostname**] und wählen Sie **Properties**. Die Anwendung scannt den Remote-Computer unter Verwendung von WMI.

5 Das Scanergebnis gibt den Status der WMI-Konnektivität zwischen dem SafeGuard PortProtector Management Server und dem Zielrechner an.

## 6.11 Vorübergehende Aufhebung des SafeGuard-Schutzes

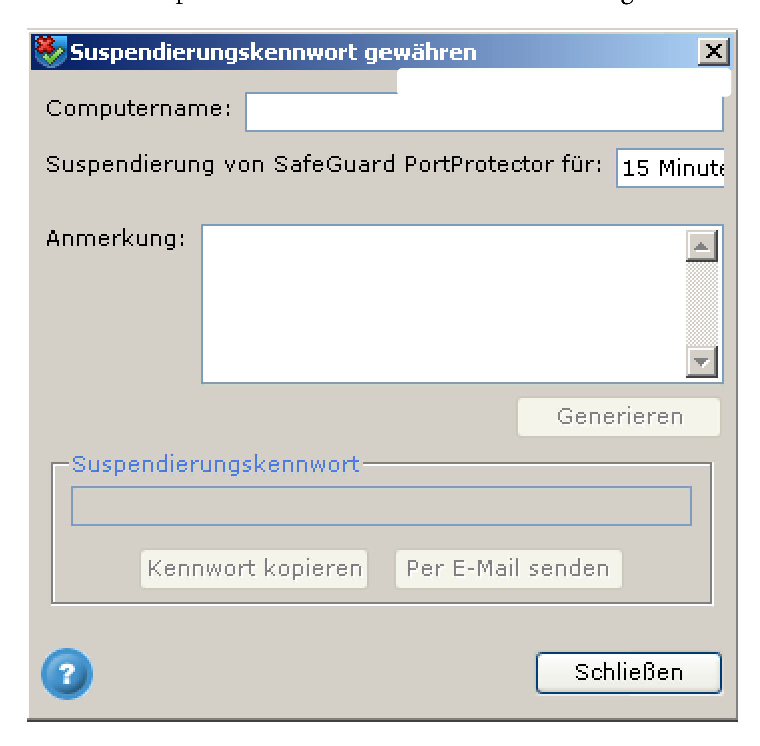
Es kann manchmal erforderlich sein, den SafeGuard-Schutz auf einem Client temporär außer Kraft zu setzen, ohne SafeGuard PortProtector Client zu deinstallieren. Das könnte beispielsweise der Fall sein, wenn ein Benutzer, der sich nicht im Büro befindet, auf einem Laptop einmalig ein nicht autorisiertes Disk-on-Key-Gerät anschließen muss, um eine wichtige Präsentation einzusehen, die sich auf diesem Disk-on-Key befindet.

Der Endbenutzer benötigt ein Kennwort, um die Suspendierung durchzuführen. Dieses Kennwort wird vom Administrator generiert und dem Benutzer zur Verfügung gestellt. Die Aufhebung beginnt, sobald der Benutzer das Kennwort eingibt, und gilt für einen voreingestellten, begrenzten Zeitraum. Sobald der Zeitraum abgelaufen ist, wird der Schutz des Clients wiederhergestellt.

Wenn der Schutz wieder hergestellt ist, werden die Client-Logs hinsichtlich der Geräte aktualisiert, die während des Suspendierungszeitraums angeschlossen wurden, und hinsichtlich der Dateien, die zu bzw. von diesen Geräten kopiert wurden.

**So öffnen Sie das Fenster *Suspendierungskennwort gewähren*:**

Klicken Sie in der Clients-Tabelle mit der rechten Maustaste auf den Computer, dessen Schutz Sie aufheben möchten, und wählen Sie **Suspendierungskennwort gewähren**. Alternativ hierzu können Sie auf die Schaltfläche **Suspendierungskennwort gewähren** in der Symbolleiste klicken, oder diese Option im Menü *Extras* wählen. Das folgende Fenster wird angezeigt:



### 6.11.1 Gewähren eines Suspendierungskennworts

Geben Sie im Fenster *Suspendierungskennwort gewähren* die erforderlichen Daten zu dem Computer ein, auf dem der Schutz aufgehoben werden soll. Geben Sie dort die Suspendierungsparameter ein und generieren Sie ein Suspendierungskennwort, das Sie dem Benutzer zur Verfügung stellen.

**So gewähren Sie ein Suspendierungskennwort:**

1 Wenn das Feld **Computername** leer ist (was der Fall sein kann, wenn Sie dieses Dialogfeld über das Menü *Extras* öffnen oder die Schaltfläche der Symbolleiste nutzen), geben Sie den gewünschten Computernamen ein.

2 Wählen Sie im Feld **Suspendierung von SafeGuard PortProtector für** den Suspendierungszeitraum aus der Dropdown-Liste.

3 Geben Sie im Feld **Anmerkungen** einen beliebigen Text ein, wie etwa eine Beschreibung des Aufhebungsgrunds (optional).

4 Klicken Sie auf **Generieren**. Das System generiert ein Kennwort und zeigt es an.

5 Klicken Sie auf **Kennwort kopieren**, um das Kennwort in die Zwischenablage zu kopieren, oder klicken Sie auf **Per E-Mail senden**, um eine neue Nachricht in Ihrem E-Mail-Programm zu öffnen, die alle Suspendierungsdaten enthält (Computername, Aufhebungszeitraum, Anmerkungen und Kennwort).

## 6.12 Zurücksetzen und Aktualisieren des Client-Status

Im Laufe der Zeit kann es vorkommen, dass zuvor geschützte Clients nicht immer geschützt bleiben. Mit dieser Option können Sie den Status von SafeGuard PortProtector Clients zurücksetzen, die in der Clients-Tabelle als 'Served' erscheinen, derzeit aber möglicherweise 'Not Served' sind.

**So setzen Sie den Status eines Clients zurück und aktualisieren ihn:**

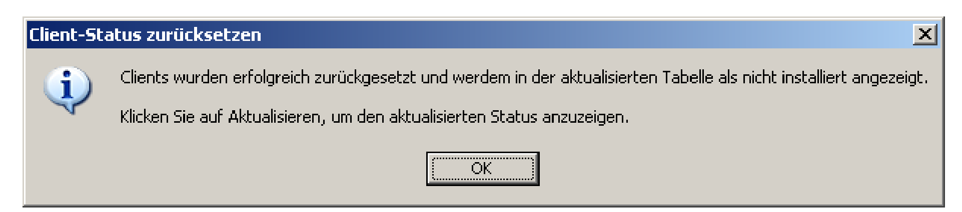
Klicken Sie in der Clients-Tabelle mit der rechten Maustaste auf den 'Bedienten' Client, den Sie zurücksetzen möchten.

ODER

1 Klicken Sie in der Organisationsstruktur mit der rechten Maustaste auf das gewünschte Objekt.

2 Ein Menü wird angezeigt.

3 Wählen Sie in dem Menü die Option **Client-Status zurücksetzen**. Das folgende Fenster wird angezeigt:



**Hinweis:** Die Option **Client-Status zurücksetzen** ist nur für 'Served' Clients aktiviert.

**Hinweis:** Sie können in der Clients-Tabelle mehrere Clients für das Zurücksetzen auswählen. Wenn Sie in der Organisationsstruktur ein Objekt auswählen (wie etwa eine Organisationseinheit oder eine Domäne), werden alle zu diesem Objekt gehörenden Clients zurückgesetzt.

4 Klicken Sie in der Symbolleiste auf **Aktualisieren**. Der Client-Status wird aktualisiert, und 'Not Served' Clients, die zuvor als 'Served' erschienen, werden jetzt mit ihrem richtigen Status (Not Served) angezeigt.

**Hinweis:** Zurückgesetzte Clients werden wieder als 'Bedient' angezeigt, sobald sie mit dem Server kommunizieren.

## 6.13 Löschen von nicht in der Domäne befindlichen Clients

Wie zuvor erläutert kann die Organisationsstruktur Clients enthalten, die nicht (mehr) zu einer der Domänen in der Organisationsstruktur gehören und in der Struktur unter Not in Domain erscheinen. Einige dieser Clients sind möglicherweise nicht mehr relevant, und Sie möchten sie vielleicht aus der Struktur löschen. Sie können entweder alle nicht in der Domäne befindlichen Clients (sowohl Served als auch Not Served) oder nur bestimmte Clients löschen.

**Hinweis:** Ein Client wird als Not in Domain hinzugefügt, sobald er mit dem Server kommuniziert und festgestellt wird, dass er nicht zu einer der Domänen in der Struktur gehört.

**So löschen Sie alle nicht einer Domäne befindlichen Clients:**

1 Klicken Sie in der Organisationsstruktur mit der rechten Maustaste auf **Nicht in Domäne**. Ein Menü wird angezeigt.

2 Wählen Sie im Menü die Option **Clients löschen**. Es wird ein Bestätigungsfenster angezeigt.

3 Klicken Sie auf **Ja**. Alle nicht in der Domäne befindlichen Clients werden gelöscht.

4 Klicken Sie in der Symbolleiste auf **Aktualisieren**. Die gelöschten Clients werden nicht mehr angezeigt.

**So löschen Sie bestimmte Clients, die nicht in einer Domäne sind:**

1 Klicken Sie in die Clients-Tabelle mit der rechten Maustaste auf den gewünschten Client (Sie können ein 'Nicht-in-Domäne'-Client unabhängig davon, ob er Served oder Not Served ist, löschen). Ein Menü wird angezeigt.

2 Wählen Sie im Menü die Option **Clients löschen** (Nicht in Domäne). Es wird ein Bestätigungsfenster angezeigt.

3 Klicken Sie auf **Ja**. Alle ausgewählten Clients, die nicht in der Domäne sind, werden gelöscht.

4 Klicken Sie in der Symbolleiste auf **Aktualisieren**. Die gelöschten Clients werden nicht mehr angezeigt.

## 6.14 Auditing von Geräten

Wenn Sie prüfen möchten, welche Geräte derzeit an Endpunkten Ihrer Organisation angeschlossen sind oder früher angeschlossen waren, können Sie dafür ein Prüfprotokoll erstellen. Das Auditing von Geräten erfolgt mittels SafeGuard PortAuditor, unserem Scan- und Auditing-Tool, das detailliert im *SafeGuard PortAuditor Benutzerhandbuch* beschrieben ist. Sie können bei Bedarf SafeGuard PortAuditor direkt von SafeGuard PortProtector aus starten.

**So starten Sie SafeGuard PortAuditor:**

Klicken Sie auf die Schaltfläche **Geräte-Audit**. Beim ersten Mal werden Sie aufgefordert, den Speicherort der Datei auditor.exe zu suchen. Danach wird SafeGuard PortAuditor gestartet und dessen Hauptfenster wird geöffnet.

# 7 Administration

## Über dieses Kapitel

Dieses Kapitel beschreibt das Fenster *Administration*, seine Parameter und die administrativen Überlegungen bei der Einrichtung von SafeGuard PortProtector.

Dieses Kapitel enthält die folgenden Abschnitte:

- ***Verwalten von SafeGuard PortProtector*** beschreibt die Situationen, in denen die Administration von SafeGuard PortProtector nötig sein kann, und wie Sie dazu das Fenster *Administration* öffnen.
- ***Fenster Administration*** beschreibt die verschiedenen Einstellungen in den sieben Registerkarten des Fensters *Administratioseinstellungen*.

## 7.1 Verwalten von SafeGuard PortProtector

Wenn SafeGuard PortProtector nach der Installation zum ersten Mal gestartet wird, wird das System mit Standardeinstellungen initialisiert, die für die Mehrheit der Benutzer anwendbar sein können.

Während des laufenden Betriebs von SafeGuard PortProtector können Sie die verschiedenen Administrationseinstellungen aktualisieren. Hierzu verwenden Sie das Fenster *Administration*, wie folgt.

**So öffnen Sie das Fenster Administration:**

Wählen Sie im Menü *Extras* die Option **Administration**

ODER

Klicken Sie in der Start-Welt im Abschnitt *Mehr* auf den Link **Administrationseinstellungen ändern**.

Das Fenster *Administration* wird angezeigt.

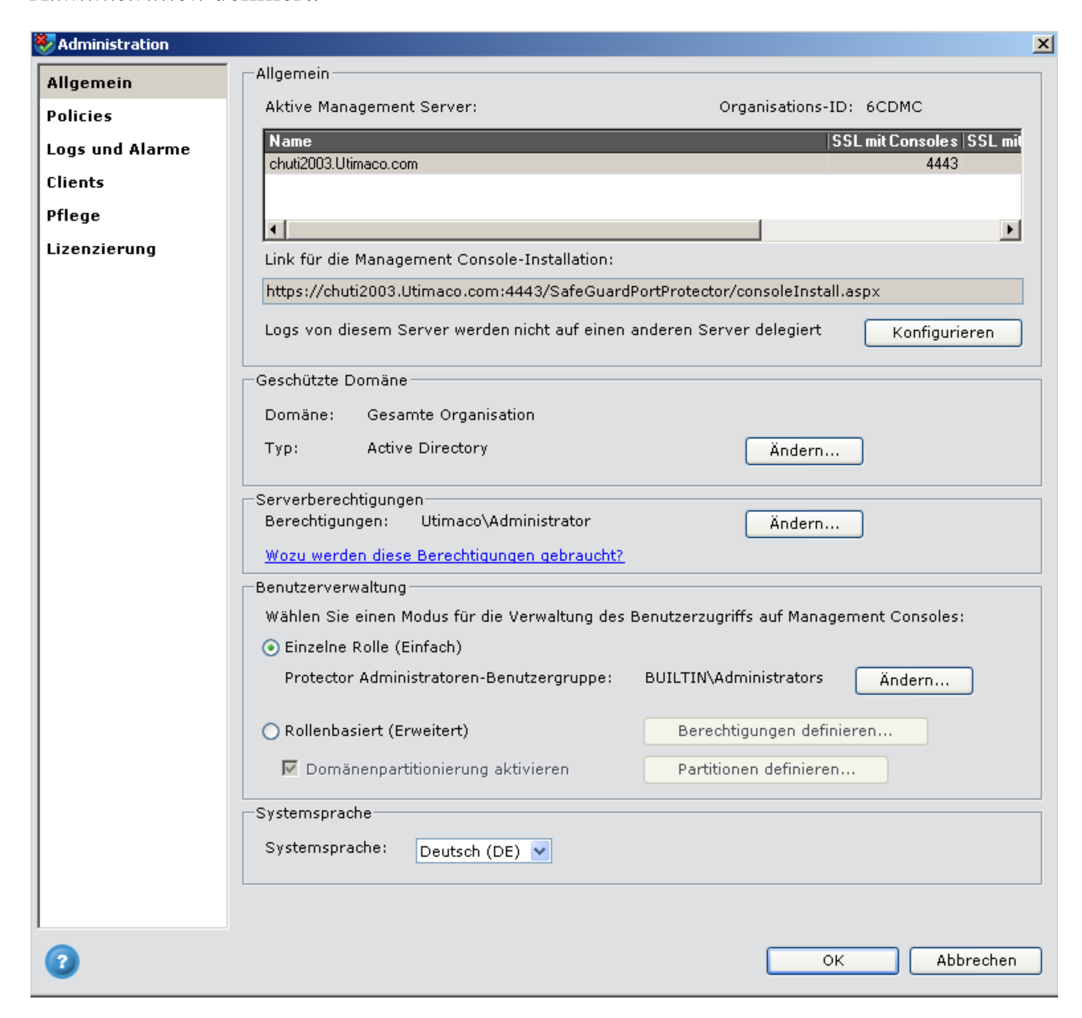
## 7.2 Fenster Administration

Die Einstellungen im Fenster *Administration* bestehen aus sechs Registerkarten:

- **Allgemein**, in *Einstellungen auf der Registerkarte Allgemein* beschrieben.
- **Policies**, in *Konfigurieren der Eigenschaften auf der Registerkarte Policies* beschrieben.
- **Logs und Alarme**, in *Konfigurieren der Einstellungen auf der Registerkarte Logs und Al beschrieben.*
- **Clients**, in *Konfigurieren der Einstellungen auf der Registerkarte Clients* beschrieben.
- **Pflege**, in *Konfigurieren der Einstellungen auf der Registerkarte Pflege* beschrieben.
- **Lizenzierung**, in *Konfigurieren der Einstellungen auf der Registerkarte Lizenzierung beschrieben.*

## 7.3 Einstellungen auf der Registerkarte Allgemein

Allgemeine Administrationseinstellungen werden auf der Registerkarte *Allgemein* des Fensters *Administration* definiert:




### 7.3.1 Konfigurieren der Einstellungen auf der Registerkarte Allgemein

Auf der Registerkarte *Allgemein* können Sie die allgemeinen Parameter der Systemkonfiguration für SafeGuard PortProtector konfigurieren. Sie enthält die folgenden Abschnitte:

- *Allgemein*
- *Log-Delegierung*
- *Serverberechtigungen*
- *Benutzerverwaltung*

**Hinweis:** Bei jeder Änderung einer der Einstellungen auf dieser Registerkarte müssen Sie unten im Fenster *Administration* auf **OK** klicken, damit die Änderungen übernommen werden.

### 7.3.1.1 Allgemein

Diese Felder enthalten Informationen zum Management Server, in dem SafeGuard PortProtector verwaltet wird. Jeder SafeGuard PortProtector Server ist ein Computer, auf dem Sie die SafeGuard PortProtector Console und den SafeGuard PortProtector Management Server installiert haben. Jede SafeGuard PortProtector Console arbeitet mit dem SafeGuard PortProtector Management Server, auf dem sie installiert wurde. Der Management Server hat mehrere Rollen:

- Er wird als Zentralstelle für die Kommunikation mit SafeGuard PortProtector Clients genutzt, die auf Endpunkten installiert sind.
- Er hält eine Datenbank mit allen Systemkonfigurationen, Policies und Logs.
- Er kommuniziert mit den Management Consoles.

#### 7.3.1.1.1 Aktive Management Server

Im Folgenden werden die Eigenschaften in diesem Abschnitt beschrieben:

- **Aktive Management Server –** Dieses Raster zeigt die aktiven SafeGuard PortProtector Management Server an.
- **Servername –** Dieses Feld zeigt den vollständigen Namen des Computers an, auf dem der SafeGuard PortProtector Server läuft. Daneben steht in Klammern eine Zeichenfolge, die den eindeutigen Verschlüsselungsschlüssel angibt, der bei der Installation generiert wurde (z. B. P8G2U). Diese Zeichenfolge dient zur Verifizierung, dass die Clients denselben Verschlüsselungsschlüssel haben, und zur Prüfung von Problemen mit dem Verschlüsselungsschlüssel. Diese Felder können nicht konfiguriert werden.
- **Server-Port –** Dieses Feld zeigt die TCP-Ports, auf denen der Management Server mit den Clients (Kontrolle und Erfassung von Logs) und mit den Management Consoles (Definieren von Policies, Überprüfung von Logs etc.) kommuniziert.

  Die gesamte Management Server-Kommunikation über diese TCP-Ports wird mit SSL verschlüsselt.

  Bei der Installation unter Windows 2003 wird Port 4443 gemäß Voreinstellung für die SSL-Kommunikation Server-Console genutzt, und Port 443 wird standardmäßig für die SSL-Kommunikation Server-Client genutzt. Bei der Installation unter Windows XP, wird Port 443 als Standardport sowohl für die SSL-Kommunikation vom Server als auch vom Client benutzt. Falls Sie die Portnummer aus irgendeinem Grunde ändern möchten, können Sie sie in den Microsoft IIS-Einstellungen auf dem Management Server-Computer ändern.

**So ändern Sie den Port:**

1. Öffnen Sie die IIS-Einstellungen in der Systemsteuerung auf Ihrem Management Server-Computer (Verwaltung → Internet Information Services).
2. Suchen Sie die SafeGuard PortProtector-Site:
   - Bei Windows XP ist das "Default Web Site"
   - Bei Windows 2003 gibt es zwei Web-Sites: "SafeGuard PortProtector Web Site" für Management Console-Kommuinikation (Standardport 4443) und "SafeGuard PortProtector Web Site WS" für Client-Kommunikation (Standardport 443)

3 Ändern Sie die SSL-Ports auf die gewünschten Ports

4 Beenden Sie den IIS-Arbeitsprozess auf Ihrem Management Server:

- Bei Windows XP ist das "aspnet_wp.exe"
- Bei Windows 2003 ist das "w3wp.exe"

5 Öffnen Sie die SafeGuard PortProtector Management Console auf Ihrem lokalen Computer und nehmen Sie irgendeine Änderung in "Global Policy Settings" vor, um die Neuveröffentlichung aller Policies zu verursachen.

**Hinweis:**

1 Da alle Clients und Management Consoles diesen Port für die Kommunikation mit dem Management Server benutzen, wird durch die Änderung des Ports die Kommunikation mit dem Server unterbrochen, bis sie über den neuen Port informiert werden.

2 Ändern Sie den Port nie während aktiver Arbeitszeiten. Wenn jetzt mehrere Management Consoles benutzt werden, wird durch die Änderung des Ports eine sofortige Unterbrechung der Verbindung zu diesen Konsolen verursacht, was zu Datenverlust führen kann.

3 SafeGuard PortProtector Clients kommunizieren mit dem Management Server über den in ihrer Policy angegebenen Kommunikationsport. Wenn Sie den Port ändern, können die Clients nicht mehr mit dem Management Server kommunizieren bis sie die neu veröffentlichen Policies erhalten.

4 Management Console-Administratoren müssen über die Portänderung informiert werden. Sie können eine der folgenden Möglichkeiten wählen:

a. Sie veranlassen, dass die Administratoren die Management Console über die Management Console Installations-Webseite neu installieren. Sie müssen sie über die neue Adresse informieren (siehe nach dieser Anmerkung).

b. Sie teilen Ihren Administratoren den neuen Port mit. Wenn sie die Management Console das nächste Mal öffnen, müssen sie ihn manuell im folgenden Fenster eintragen:



### 7.3.1.1.2 Link für die Management Console-Installation

Normalerweise werden Management Consoles über eine Webseite auf den Management Server-Computern installiert, so dass die Benutzer das Installationspaket für die Management Console herunterladen und auf ihrem Computer installieren können.

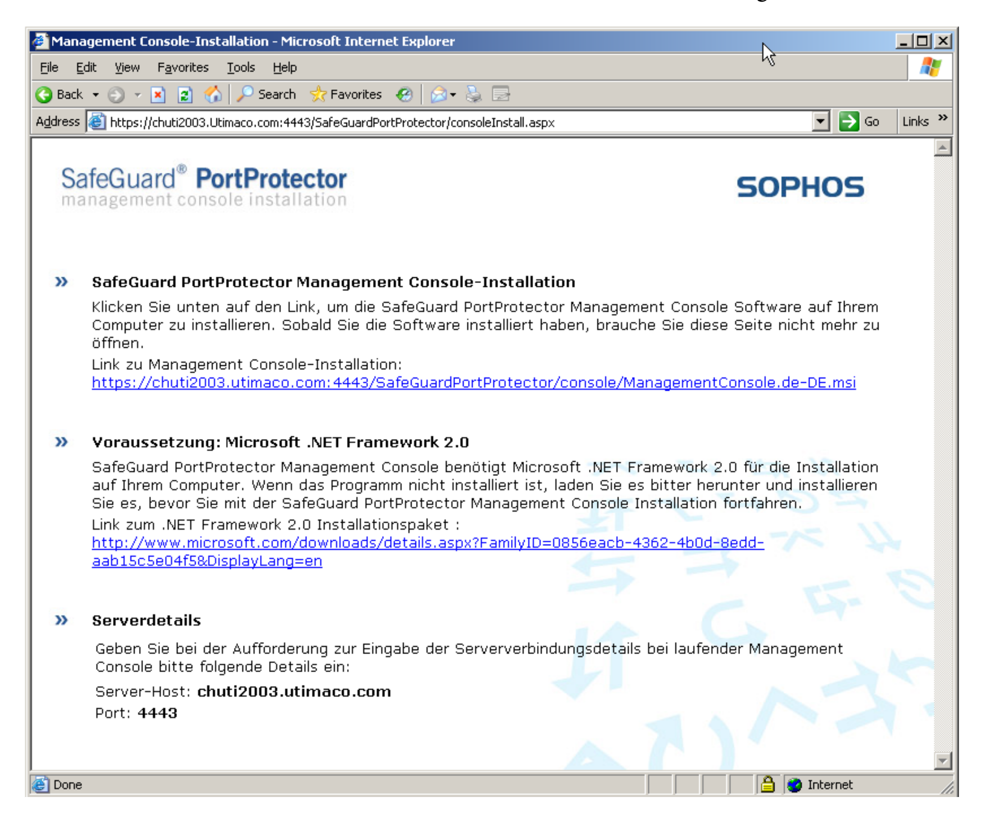
Der Link steht im folgenden Format:

https://<servername>:<serverport>/SafeGuardPortProtector/consoleinstall.aspx

**Hinweis:** Sie können auch ein kürzeres Link-Format verwenden:

https://<servername>:<serverport>/SafeGuardPortProtector

Um die Management Console auf einem neuen Computer zu installieren, brauchen Sie lediglich dem Benutzer die Adresse dieser Webseite mitzuteilen. Das folgende Fenster wird angezeigt:




**Hinweis:** Sie können auch das Installationspaket selbst verwenden, um die Management Console zu installieren. Dieses Paket ist auch auf Ihrer CD unter dem Namen ManagementConsole.msi vorhanden.

### 7.3.1.2 Log-Delegierung

**Hinweis:** Wenn Sie beabsichtigen, diese Funktion einzusetzen, beraten Sie sich vorher mit dem Sophos Support, um sicherzustellen, dass das wirklich die richtige Architektur für Ihre Umgebung ist.

Mit dieser Funktion ist es möglich, in einem einzelnen Management Server die Logs von anderen Management Servern zu sehen.

**Hinweis:** Hier einige wichtige Punkte zur Beachtung:

1 Alle Server müssen mit denselben Verschlüsselungsschlüsseln installiert werden (mittels der Option *Wiederherstellen* während Server-Installation).

2 Der Delegationsserver darf nur zur Anzeige der Logs von anderen Servern und nicht zur Anwendung von Policies oder Verwaltung von Clients benutzt werden. Empfohlen wird eine rollenbasierte Benutzerverwaltung (siehe *Benutzerverwaltung*) und ein Benutzer mit nur Rechten als Log-Reviewer.

3 Es wird empfohlen, diese Option nur dann zu nutzen, wenn die Umgebung über mehrere Domänenwälder verfügt.

**So konfigurieren Sie die Log-Delegierung:**

1 Wählen Sie auf dem Ziel-Server (Delegationsserver) in der Management Console die Option **Administration** im Menü Extras.

2 Klicken Sie oben auf der Registerkarte Allgemein auf die Schaltfläche **Konfigurieren** neben “Logs von diesem Server werden nicht auf einen anderen Server delegiert”. Das Fenster *Einstellungen für Log-Delegierung* wird angezeigt.




3 Kopieren Sie die URL in das Feld *Lokale Delegierung URL*, und speichern Sie sie in einer Datei, damit sie auf bei den auf anderen Computern installierten delegierenden Servern genutzt werden kann.

4 Öffnen Sie bei jedem der Server, deren Logs gelesen werden, in der Management Console das Fenster der Einstellungen für Log-Delegierung.

5 Wählen Sie bei *Delegierungsstatus* die Option **Log-Delegierung aktivieren**.

6 Kopieren Sie die URL vom Ziel-Server in das Feld *Ziel-Delegierung URL*.

7 Klicken Sie auf die Schaltfläche **Validieren**, um diese URL zu validieren. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern.

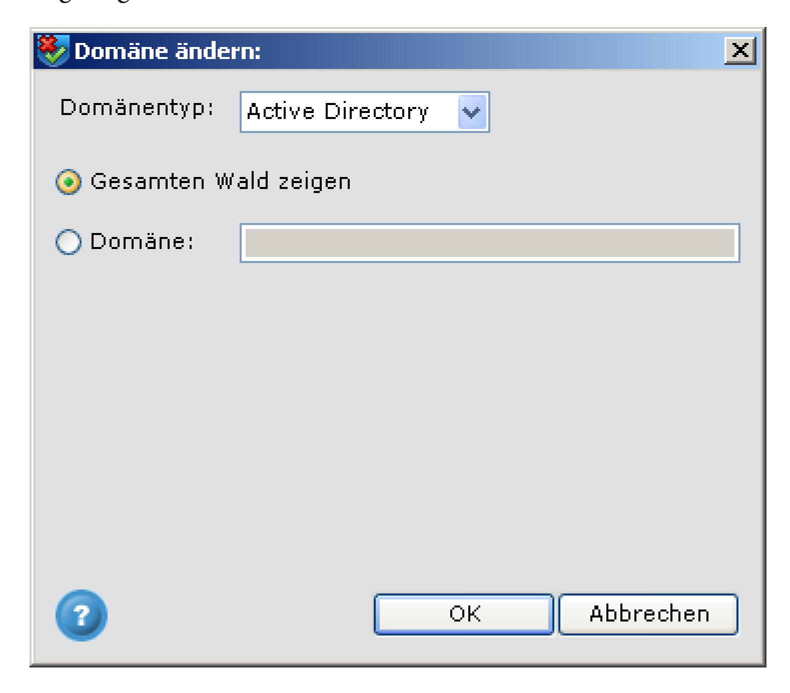
Ab diesem Zeitpunkt wird eine Kopie aller Client- und Datei-Logs von diesen Servern an den Ziel-Server gesendet.

### 7.3.1.3 Geschützte Domäne

Dieser Abschnitt definiert die geschützte Domäne, und gibt an, ob es sich um eine Active Directory- oder eine Novell eDirectory-Domäne handelt. Diese Definitionen werden im Fenster *Domäne ändern* festgelegt.

**So öffnen Sie das Fenster *Domäne ändern*:**

Klicken Sie im Abschnitt Geschützte Domäne auf **Ändern**. Das Fenster *Domäne ändern* wird angezeigt:




Definieren Sie die gewünschten Einstellungen wie unten in *Definieren einer geschützten Domäne* erläutert.

#### 7.3.1.3.1 Definieren einer geschützten Domäne

In diesem Fenster definieren Sie die geschützte Domäne und ihren Typ.

**So definieren Sie den Domänentyp:**

1 Wählen Sie im Menü *Domänentyp* die Option **Active Directory** oder **Novell eDirectory**.

2 Klicken Sie auf die entsprechende Optionsschaltfläche, um mit **Gesamten Wald zeigen** oder **Domäne** anzugeben, ob sie alles oder nur eine bestimmte Domäne anzeigen möchten. Wenn Sie eine bestimmte Domäne anzeigen möchten, geben Sie ihren Namen ein.

3 Klicken Sie zum Speichern und Beenden auf **OK**.

### 7.3.1.4 Server-Berechtigungen

Damit die Management Server-Anwendung seine Funktion im Netz ausführen kann, ist ein Benutzerkonto mit ausreichenden Rechten erforderlich.

Dieser Benutzer wird während der Installation des Management Servers definiert und ist für den reibungslosen Betrieb des gesamten Systems immens wichtig.

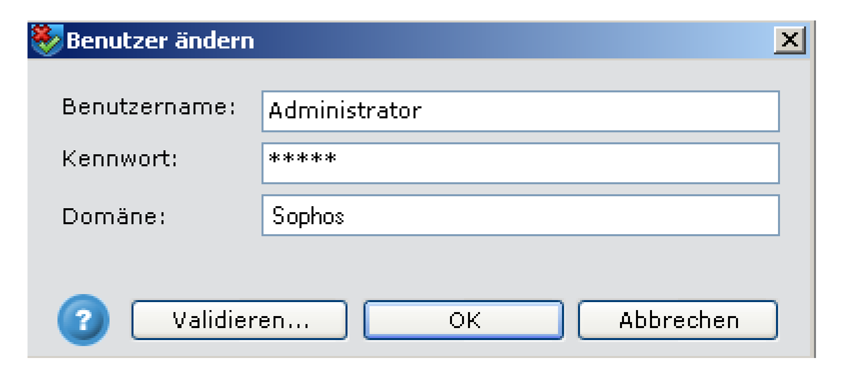
Hier die Berechtigungen, über die dieses Benutzerkonto verfügen muss:

- Erstellen von GPOs in Active Directory – Jedes Mal, wenn eine Policy erzeugt oder modifiziert wird, veröffentlicht der Management Server sie als GPO in Ihrem Active Directory.
- WMI-Zugriff auf Remote-Computer – Kontrollmeldungen vom Management Server werden über WMI an die Endpunkte gesendet. Der Benutzer muss auf jedem der Endpunkte über die Berechtigung zum WMI-Zugriff verfügen.

**Hinweis:**

1. Sophos empfiehlt, dass Sie ein Konto mit Domänen-Administratorrechten in Ihrem Netz verwenden, um Probleme zu vermeiden.
2. Wenn Sie irgendwann den "Client Installation Folder"(siehe unten) ändern oder Policies als.reg-Dateien in einem Ordner installieren möchten, müssen Sie sicherstellen, dass dieser Benutzer volle Zugriffsrechte (Lesen und Schreiben) auf diese Ordner hat.
3. Wenn Sie Policies nur als.reg-Dateien veröffentlichen, braucht dieser Benutzer nicht dazu befugt zu sein, GPOs in Active Directory zu erzeugen.

Ändern Sie bei Bedarf diesen Benutzer, indem Sie auf **Ändern** im Abschnitt *Geschützte Domäne* klicken. Das Fenster *Benutzer ändern* wird angezeigt:




#### 7.3.1.4.1 Ändern eines Benutzers

1. Geben Sie die Berechtigungen (Benutzername, Kennwort, Domäne) des neuen Benutzerkontos ein.
2. Sie können auch überprüfen, ob der Benutzer gültig ist und über ausreichende Rechte verfügt. Klicken Sie hierzu auf **Validieren**. Weitere Informationen zu diesem Benutzer finden Sie in *Server-Berechtigungen*.

**Hinweis:** Mit der Schaltfläche **Validieren** wird nur die Existenz des Benutzers in Ihrem Active Directory überprüft. Damit der Management Server ordnungsgemäß funktioniert, müssen Sie sicherstellen, dass dem Domänenbenutzer alle erforderlichen Berechtigungen zugewiesen sind.

#### 7.3.1.5 Benutzerverwaltung

Der Zugriff auf die Management Console seitens der Benutzer ist aus Sicherheitsgründen eingeschränkt. SafeGuard PortProtector braucht keine eigenen Benutzer und keine Computer-Datenbank. Stattdessen werden Berechtigungen mit Hilfe von Windows/Active Directory geprüft.

**Hinweis:** Wenn SafeGuard PortProtector mit Novell eDirectory synchronisiert ist, können nur lokale Benutzer auf dem Management Server genutzt werden.

Sie können einen der folgenden Betriebsmodi wählen:

- *Einzelne Rolle (einfach*) – Mit diesem Modus schränken Sie den Zugriff auf die Management Console auf autorisierte Benutzer ein. Alle autorisierten Benutzer können alle Aufgaben in der Console ausführen (Policies erstellen, Logs lesen, Clients suspendieren etc.).
- *Rollenbasiert (erweitert)* – Mit diesem Modus können Sie eine weitere Ebene der Zugangskontrolle anwenden, indem Sie die Benutzer entsprechend ihren Rollen auf eine Untergruppe von Funktionen innerhalb der Management Console und auf bestimmte Container einer Organisation einschränken, für die sie verantwortlich sind.

Der Standardmodus nach der Installation ist: Einzelne Rolle (einfach).

##### 7.3.1.5.1 Einzelne Rolle (einfach)

###### 7.3.1.5.1.1 Mit mehreren Management Consoles arbeiten

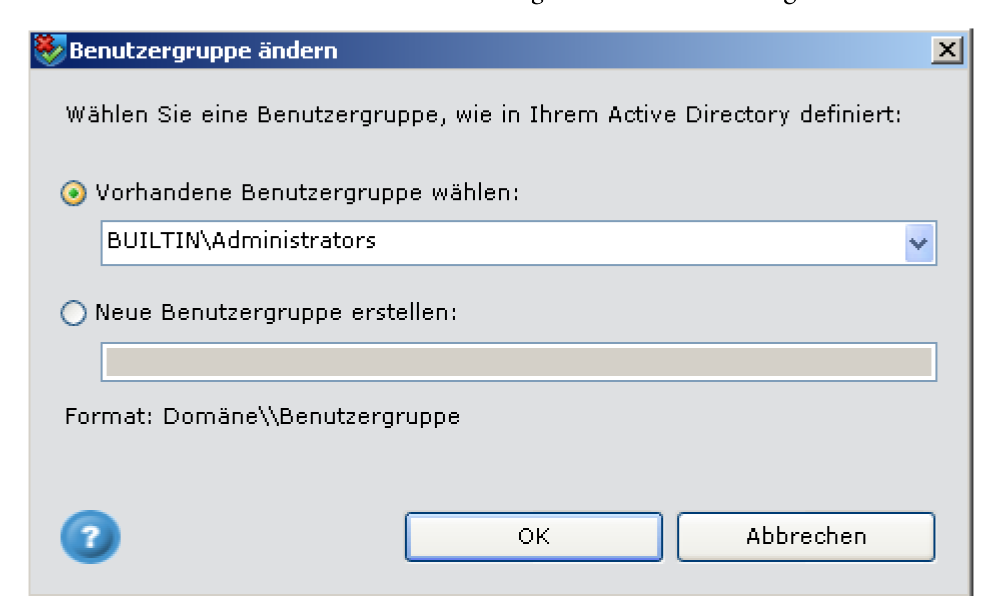
Der Modus "Einzelne Rolle" ist darauf ausgelegt, mehreren Management Consoles jeweils mit eigenem Benutzernamen und Kennwort den Zugriff auf den Management Server zu gestatten. Dazu wird überprüft, ob der Benutzer ein Mitglied er Benutzergruppe ist, die als "Protector Administrators User Group" definiert wurde.

Standardmäßig ist diese Eigenschaft nach der Installation des Management Servers auf "BUILTIN\Administrators" gesetzt. Dadurch wird der Zugriff auf die lokalen Administratoren des Server-Computers eingeschränkt.

Wenn Sie mehrere Administratoren für die SafeGuard PortProtector Management Console planen, wird empfohlen, dass Sie hier eine Benutzergruppe aus Ihrem Active Directory festlegen und die entsprechenden Administratoren als Mitglieder dieser Benutzergruppe hinzufügen. Hierfür benutzen Sie das Fenster *Benutzergruppe ändern*.

**So öffnen Sie das Fenster *Benutzergruppe ändern*:**

Klicken Sie im Abschnitt *Benutzerverwaltung* auf **Ändern**. Das folgende Fenster wird angezeigt:




#### 7.3.1.5.1.2 Ändern der Administrators-Benutzergruppe

Im Fenster *Benutzergruppe ändern* definieren Sie die entsprechende Benutzergruppe.

**So ändern Sie die Benutzergruppe:**

1. Wählen Sie eine der vorhandenen Benutzergruppen aus der Dropdown-Liste, oder legen Sie eine neue Benutzergruppe an. Verwenden Sie beim Erstellen einer neuen Gruppe das folgende Format:
   Domäne\Benutzergruppe (z. B. sophos\administratoren).
   Wenn Sie die Domäne nicht eingeben, wird die Gruppe auf dem Computer angelegt, auf dem sich der SafeGuard PortProtector Management Server befindet.

2. Klicken Sie auf **OK**.

**Hinweis:** Eine neue Benutzergruppe wird nur einmal angelegt, nachdem Sie die Änderungen im Fenster Administration bestätigt und auf **OK** geklickt haben.

### 7.3.1.5.2 Rollenbasiert (erweitert)

Um festzustellen, wie die Option Rollenbasiert (erweitert) funktioniert, können Sie Folgendes konfigurieren:

- ***Definieren von Berechtigungen*** – Mit diesem Modus können Sie eine weitere Ebene der Zugangskontrolle anwenden, indem Sie die Benutzer auf eine Untergruppe von Funktionen innerhalb der Management Console einschränken.
- ***Definieren von Domänenüpartitionen*** – Mit dieser Option ist die Partitionierung der der Container einer Organisation möglich, so dass darauf nur von den SafeGuard PortProtector Console-Administratoren zugegriffen werden kann, die für deren Bearbeitung verantwortlich sind.

###### 7.3.1.5.2.1 Definieren von Berechtigungen

Mit diesem Modus wird eine weitere Ebene der Zugangskontrolle angewandt, indem die Benutzer auf eine Untergruppe von Funktionen innerhalb der Management Console eingeschränkt werden. Sie können mehrere Benutzerrollen anlegen und jede auf bestimmte Funktionen in der Console beschränken.

Zum Beispiel: Sie können eine Rolle als "Logs Reviewer" definieren, die die Benutzer nur auf die Logs-Welt beschränken würde, ohne dass sie die Möglichkeit haben, Policies anzuzeigen oder zu bearbeiten. Auf die gleiche Weise können Sie eine Rolle als "Policy Administrators" definieren, die den Benutzer auf die Policies-Welt beschränkt, ohne dass er Logs anzeigen kann.

Darüber hinaus können Sie "Read Only" Benutzer definieren, die Informationen in der Management Console lediglich anzeigen und keine Änderungen vornehmen können.

Eine "Rolle" ist im Grunde ein Satz von Berechtigungen, die mit einer Benutzergruppe in Ihrem Active Directory verknüpft sind. Wenn ein Benutzer versucht, auf die Management Console zuzugreifen, werden seine Credentials (d. h. Anmeldeinformationen) mit der Domäne verglichen, und es wird die Liste der Gruppen abgerufen, bei denen er ein Mitglied ist. Der Benutzer wird autorisiert, die Funktionen auszuführen, die in den Rollen definiert sind, denen er zugewiesenen ist.

Zum Beispiel: Wenn der Benutzer sowohl ein Mitglied der Gruppe "Policy Administrators" und "Logs Reviewer" aus obigem Beispiel ist, kann er sowohl auf die Logs-Welt als auch die Policies-Welt zugreifen.

Rollen werden im Fenster *Berechtigungen definieren* definiert.

**So öffnen Sie das Fenster *Berechtigungen definieren*:**

Klicken Sie auf **Berechtigungen definieren.** Das Fenster *Berechtigungen definieren* wird angezeigt:



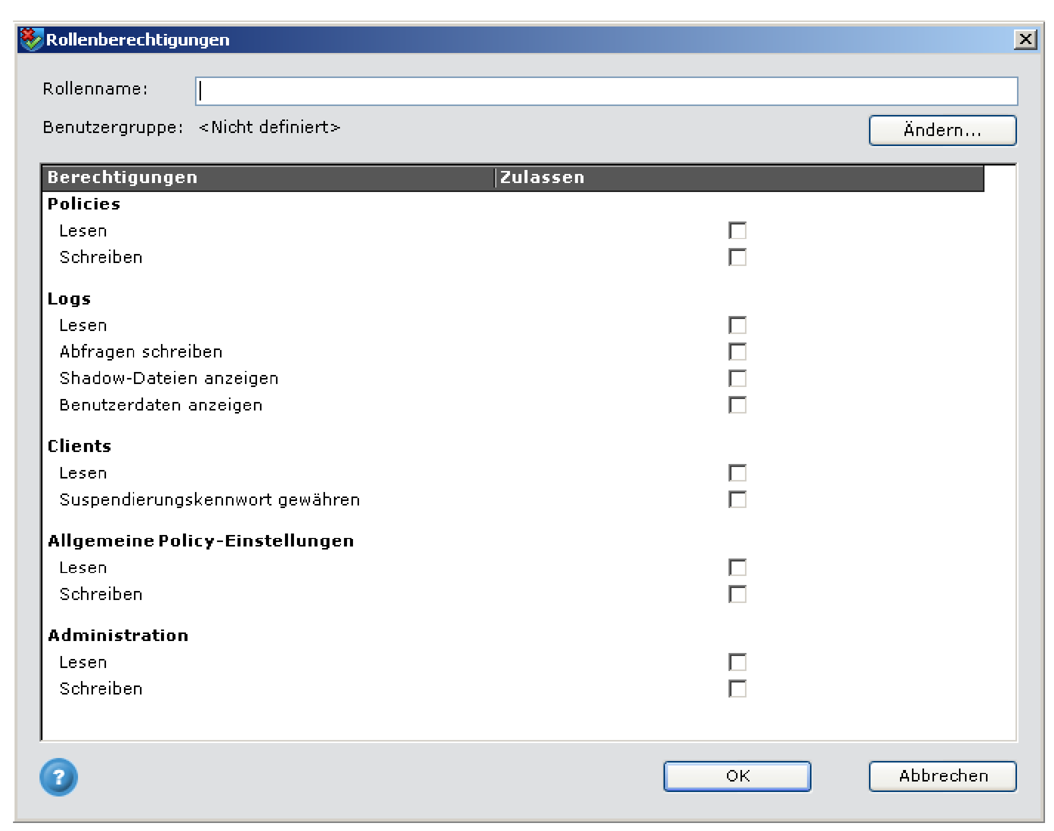
#### 7.3.1.5.2.2 Definieren von Rollen

Dieses Fenster zeigt eine Liste der vorhandenen Rollen. Sie können hier neue Rollen anlegen oder vorhandene Rollen bearbeiten bzw. löschen. Jede Zeile zeigt eine Rolle, die mit ihr verknüpfte Benutzergruppe und die Domänenpartition, der sie zugewiesen ist, an (siehe *Definieren von Domänenpartitionen*).

Die folgenden Rollen sind in SafeGuard PortProtector integriert: Super Administrator, Policy Administrator, Log Reviewer, Client Administrator. Wenn Sie eine der letzten drei Rollen benutzen möchten, können Sie sie einfach mit **Bearbeiten** bearbeiten und mit einer Benutzergruppe verknüpfen. Wenn Sie sie nicht verwenden möchten, können Sie sie mit **Löschen** löschen.

**Hinweis:** Die Rolle "Super Administrator" kann nicht bearbeitet oder gelöscht werden. Diese Rolle ist durch die Installation des Management Servers voreingestellt und hat alle Berechtigungen, einschließlich der Möglichkeit, Administrationseinstellungen zu bearbeiten. Die mit dieser Rolle verknüpfte Benutzergruppe wird aus der Gruppe abgeleitet, die im "Single Rolle"-Modus definiert ist.

Um eine neue Rolle anzulegen, klicken Sie auf **Neu**. Um eine vorhandene Rolle zu bearbeiten, klicken Sie auf **Bearbeiten**. Das folgende Fenster wird angezeigt:



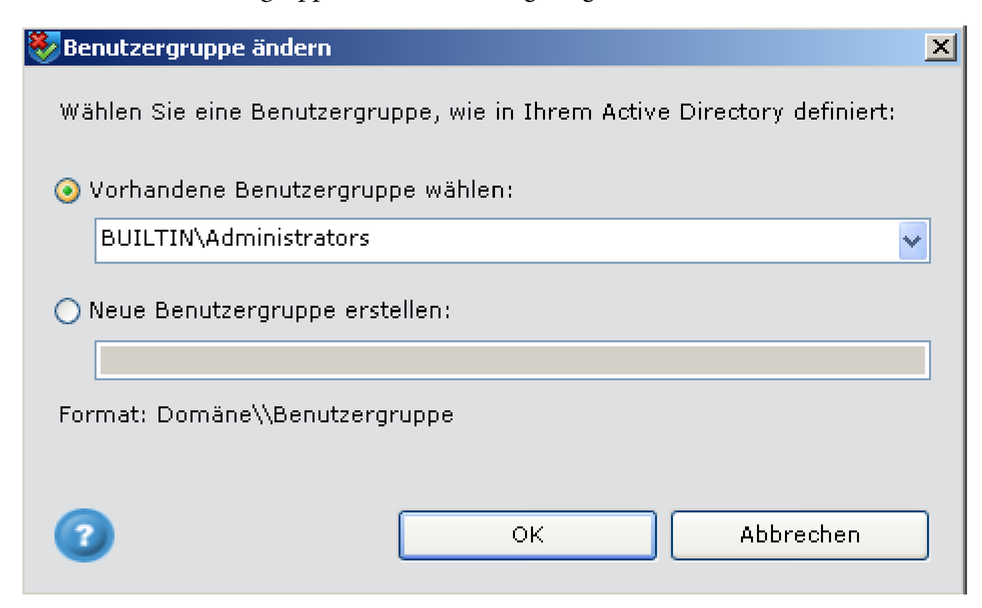

Eine Erläuterung der Definition von Rollenberechtigungen finden Sie in *Definieren von Rollenberechtigungen*.

#### 7.3.1.5.2.3 Definieren von Rollenberechtigungen

**So definieren Sie Rollenberechtigungen:**

1 Wenn es sich um eine neue Berechtigung handelt, geben Sie den Namen der Rolle bei **Rollenname** ein.

2 Wenn Sie die Benutzergruppe definieren oder ändern möchten, klicken Sie auf **Ändern**. Das Fenster *Benutzergruppe ändern* wird angezeigt:




3 Eine Erläuterung dieses Fensters finden Sie in *Ändern der Administrators-Benutzergruppe.*

**Hinweis:** Sie müssen eine Benutzergruppe auswählen, um eine Rollendefinition nutzen zu können.

**Hinweis:** Wenn Sie Novell einsetzen, können Sie nur eine lokale Benutzergruppe auf dem Management Server benutzen.

4 Mit der Funktion Domänenpartitionierung ist die Partitionierung der Container einer Organisation möglich, so dass darauf nur von den SafeGuard PortProtector Console-Administratoren zugegriffen werden kann, die für deren Bearbeitung verantwortlich sind. Diese Funktion beeinflusst fast alle Aspekte von der SafeGuard PortProtector-Oberfläche, so dass nur die Container in der SafeGuard PortProtector Console angezeigt werden, die mit der Domänenpartition verknüpft sind, die dem SafeGuard PortProtector-Benutzer zugewiesen ist.

**Hinweis:** Die Rollenberechtigungen legen fest, **welche administrativen Maßnahmen** die einzelnen SafeGuard PortProtector-Administratoren ausführen können. Die Einstellungen der Domänenpartition definieren die **Clients, auf denen** sie diese Aktionen ausführen können.

Um die Partition für diese Rollenberechtigung zu ändern, wählen Sie in der Dropdown-Liste **Domänenpartition** eine andere Partition. Wenn Sie eine neue Domänenpartition definieren wollen, klicken Sie auf **Neue Partition.** Um eine vorhandene Domänenpartition zu bearbeiten, klicken Sie auf **Partition bearbeiten.** Um die Partition für diese Rollenberechtigung zu ändern, wählen Sie in der Dropdown-Liste **Domänenpartition** eine andere Partition.

5 Bearbeiten Sie die Berechtigungen, indem Sie die **Allow**-Kontrollkästchen aktivieren bzw. deaktivieren. Jedes Kontrollkästchen, das Sie zulassen, gibt der Benutzergruppe die Berechtigung 'zugelassen'.

6 Klicken Sie auf **OK**.

###### 7.3.1.5.2.4 Definieren von Domänenpartitionen

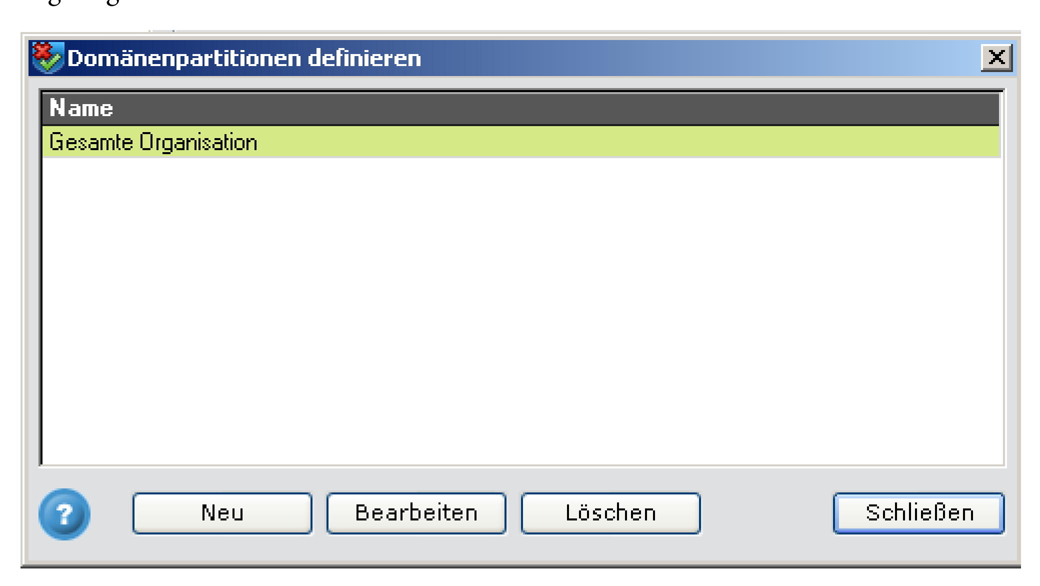
Mit SafeGuard PortProtector Domänepartitionierung ist die Partitionierung der der Container einer Organisation möglich, so dass darauf nur von den SafeGuard PortProtector Console-Administratoren zugegriffen werden kann, die für deren Bearbeitung verantwortlich sind. Die Domäne Ihrer Organisation kann gemäß ihrer Organisationsstruktur partitioniert werden, und den einzelnen Domänenpartitionen können dann verschiedene SafeGuard PortProtector-Administratoren zugeordnet werden.

**Hinweis:** Die Domänenpartitionierung ist besonders beim Datei-Shadowing von Bedeutung. Beim File-Shadowing werden verborgene Kopien von Dateien erfasst, die zu/von externen Speichergeräten verschoben wurden; deshalb möchten Sie unter Umständen den Zugriff auf diese sensiblen Dateien einschränken, indem Sie definieren, welcher Administrator gemäß der Organisationseinheit oder der Herkunft der Datei berechtigt ist, eine Shadow-Datei zu sehen.

Markieren Sie das Kontrollkästchen **Enable Compartmentalization**, um die Funktion der Domänenpartitionierung zu aktivieren, mit der Sie Domänenpartitionen auf Rollen aufteilen können. Dann können Sie das Fenster die *Domänenpartitionen definieren* öffnen, wie nachfolgend beschrieben.

**So öffnen Sie das Fenster *Domänenpartitionen definieren*:**

Klicken Sie auf **Partitionen definieren.** Das Fenster *Domänenpartitionen definieren* wird angezeigt:

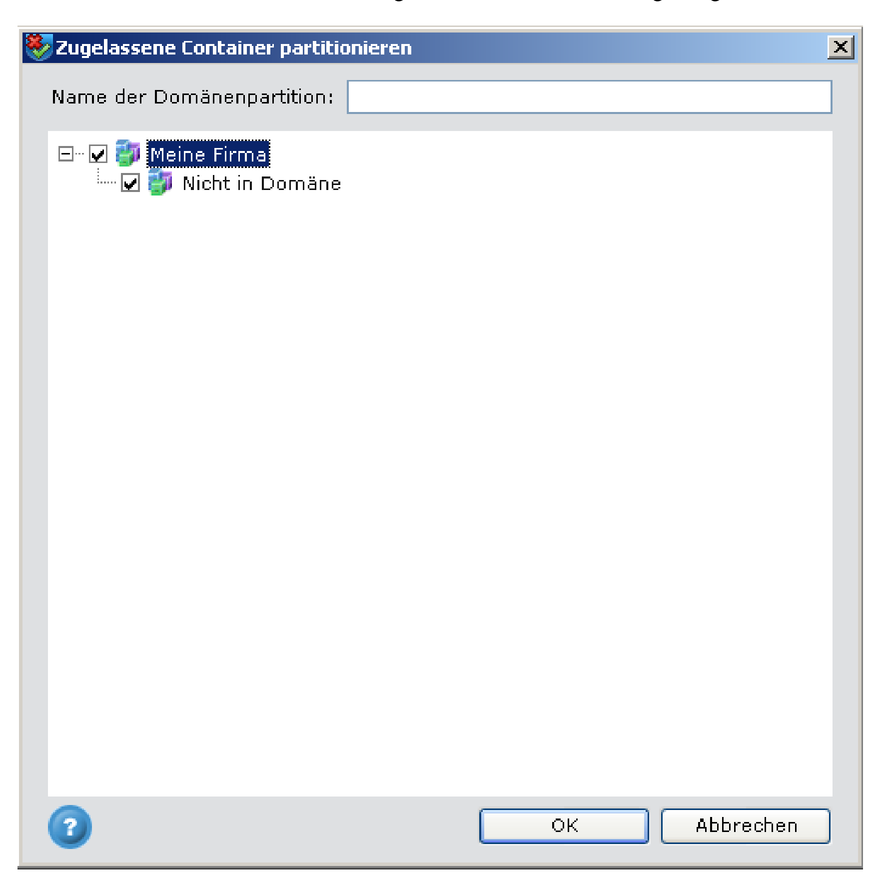



Dieses Fenster zeigt eine Liste der vorhandenen Domänenpartitionen. Sie können hier neue Domänenpartitionen anlegen oder vorhandene Domänenpartitionen bearbeiten bzw. löschen.

Um eine vorhandene Domänenpartition zu bearbeiten, klicken Sie auf **Bearbeiten**.

**So erstellen Sie eine neue Domänenpartition:**

1 Klicken Sie auf **Neu.** Das folgende Fenster wird angezeigt:




2 Geben Sie den Namen für die Domänenpartition oben im Fenster ein.

3 Markieren Sie die Kontrollkästchen der Container, die in dieser Domäne enthalten sein sollen. Dazu müssen Sie evtl. die Struktur erweitern, um die auszuwählenden Container sehen zu können.

4 Klicken Sie auf **OK.** Diese Domänenpartition wird im Feld **Domänenpartition** im Fenster *Rollenberechtigungen* zur Auswahl angeboten, wie in *Definieren von* Rollen beschrieben. Um diese Partition mit einer Gruppe von Benutzern zu verknüpfen, müssen Sie sie im Fenster *Rollenberechtigungen* mit einer Benutzerrolle verknüpfen.

#### 7.3.1.6 Systemsprache

SafeGuard PortProtector ermöglicht es Ihnen, Ihre eigene Sprache einzustellen. Mit jeder neuen Version kommen weitere Sprachen hinzu.

Die Sprache beeinflusst Folgendes:

- Die Sprache für die Menüs und Schaltflächen der Management Console
- Die Sprache der Textfelder in den Logs
- Die Sprache für standardmäßige Endbenutzer-Meldungen

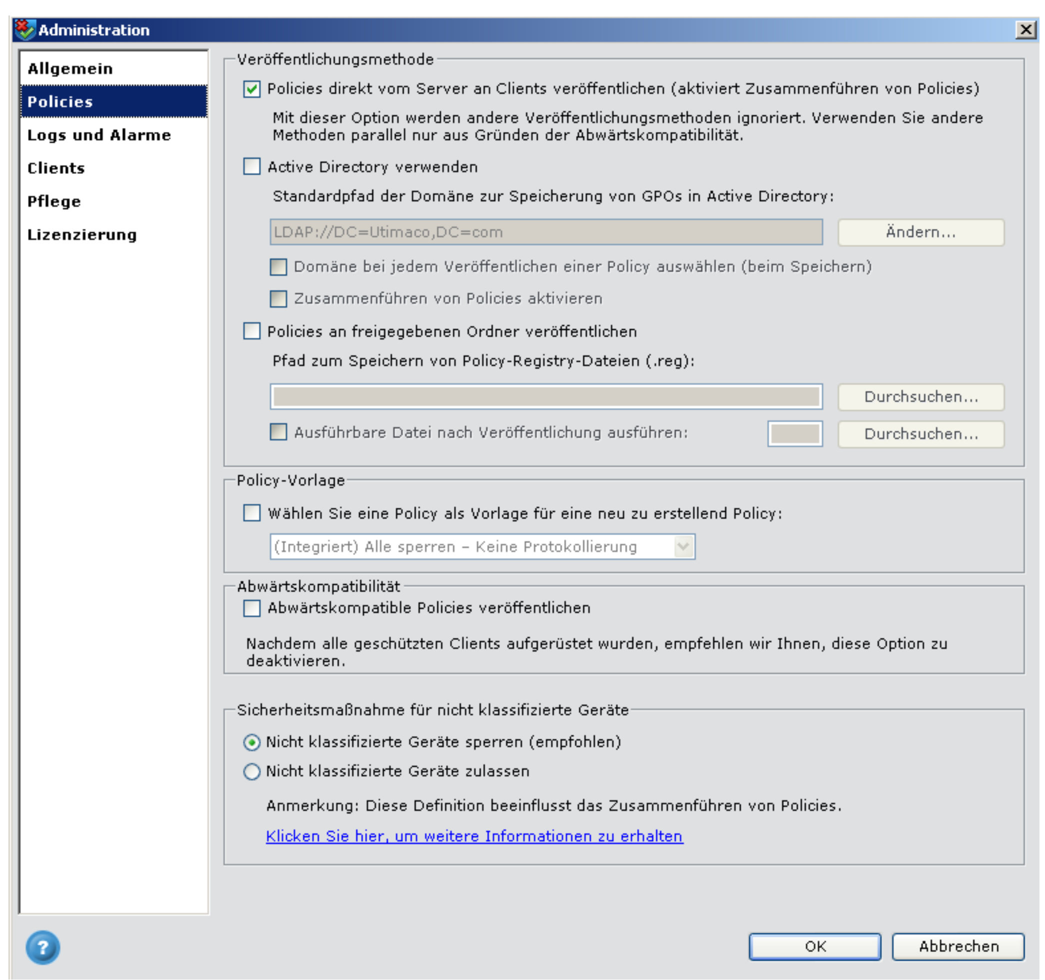
Die Systemsprache wird normalerweise während der Installation des Management Servers definiert. Wenn Sie sie nach der Installation ändern möchten, legen Sie sie hier fest.

**Hinweis:**

1. Nachdem Sie die Sprache geändert haben, müssen Sie die Management Console neu starten, damit die Sprachänderung wirksam wird.
2. Sie können nicht mehrere Consoles in verschiedenen Sprachen laufen lassen.
3. Logdaten, die vor der Sprachänderung gespeichert wurden, werden in der vorherigen Sprache angezeigt.
4. Die Sprache für SafeGuard PortProtector Clients wird während der Installation der Clients definiert (siehe *SafeGuard PortProtector Installationshandbuch*).

## 7.4 Konfigurieren der Einstellungen auf der Registerkarte Policies

Policy-Administrationseinstellungen werden auf der Registerkarte *Policies* des Fensters *Administration* definiert:




### 7.4.1 Policies-Einstellungen

Auf der Registerkarte *Policies* können Sie Konfigurationsparameter hinsichtlich der Policies in Policies in SafeGuard PortProtector konfigurieren. Sie enthält die folgenden Abschnitte:

- *Veröffentlichungsmethode*
- *Policy-Vorlage*
- *Abwärtskompatibilität*
- *Sicherheitsmaßnahme für nicht klassifizierte Geräte*

**Hinweis:** Bei jeder Änderung einer der Einstellungen auf dieser Registerkarte müssen Sie unten im Fenster *Administration* auf **OK** klicken, damit die Änderungen in Kraft treten.

#### 7.4.1.1 Veröffentlichungsmethode

SafeGuard PortProtector bietet drei Methoden zur Verteilung von Policies (siehe auch *Kapitel 4, Verteilen von Policies*:

- **Unter Verwendung des Policy Servers**: Mit dieser Option können Sie Policies in der Management Console mit Organisationsobjekten verknüpfen und sie direkt vom Management Server an die Clients verteilen.
- **Unter Verwendung von Active Directory:** Bei dieser Option wird der standardmäßige GPO-Verteilungsmechanismus von Active Directory zur Verteilung von Policies genutzt.
- **Unter Verwendung einer Registry-Datei in einem freigegebenen Ordner:** Diese Option speichert Registry-Dateien in einem freigegebenen Ordner, die dann mit Hilfe von Drittanbieter-Tools an SafeGuard PortProtector Clients verteilt werden können, wie weiter unten beschrieben.

Die Standardeinstellung nach der Installation ist die Veröffentlichung von Policies unter Verwendung des Policy Servers. Wenn Sie diese Option tatsächlich nutzen, verwenden Sie die anderen Verteilungsmethoden nur zusätzlich aus Gründen der Abwärtskompatibilität.

Wenn Sie mehrere dieser Optionen wählen, werden SafeGuard PortProtector-Policy-Dateien an die entsprechenden Stellen kopiert, und es kann jede beliebige Methode zur Verteilung der Policies an SafeGuard PortProtector Clients genutzt werden.

Wenn Sie keine dieser Optionen wählen, werden SafeGuard PortProtector-Policies nur in der SafeGuard PortProtector-Policy-Datenbank gespeichert. Nachdem Sie eine dieser Optionen aktiviert haben, werden diese Policies an die entsprechenden Stellen kopiert.

Auch wenn die meisten Benutzer normalerweise die Methode für die Policy-Verteilung ein Mal nach der Installation definieren, können Sie diese Einstellungen doch jederzeit ändern. Bei jeder Änderung generiert die Anwendung alle Policies an den aktualisierten Standorten neu. Siehe *Kapitel 4, Verteilen von Policies*.

**Policy Server**

Wählen Sie die Option **Policy direkt vom Server an Clients veröffentlichen**, um den Policy Server zu nutzen. Dadurch können Sie Policies in der Management Console mit Organisationsobjekten verknüpfen und sie direkt vom Management Server an die Clients verteilen. Mit dieser Option werden alle Policies zusammengeführt, wenn mehrere Policies mit einem Organisationsobjekt verknüpft ist (siehe Zusammenführen von Policies im Kapitel *Verteilen von Policies*). Wenn Sie diese Option nutzen, können die anderen Optionen weiterhin ausgewählt werden. Verwenden Sie die anderen Verteilungsmethoden jedoch nur zusätzlich aus Gründen der Abwärtskompatibilität.

**Active Directory**

Wählen Sie die Option **Active Directory verwenden**, um anzugeben, dass SafeGuard PortProtector-Policies als GPOs gespeichert und dann automatisch mit Hilfe des standardmäßigen Microsoft GPO-Verteilungsmechanismus verteilt werden. In diesem Fall erzeugt SafeGuard PortProtector automatisch jede Policy, die Sie in der Policies-Welt definieren, als GPO in Active Directory. Diese Policies werden dann automatisch von Active Directory an die Organisationseinheiten verteilt, denen die GPOs zugewiesen wurden.

Weitere Informationen finden Sie im Kapitel *Verteilen von* Policies.

**Hinweis:** Wenn Sie zuvor die Option **Policies an freigegebenen Ordner veröffentlichen**, weiter unten beschrieben, ausgewählt haben und dann die Option **Active Directory verwenden** wählen (und die Option **Freigegebener Ordner** deaktivieren), werden alle vorhandenen Policies nach Active Directory kopiert. Ab diesem Zeitpunkt werden alle Policies nur von Active Directory gehandhabt. Dieser Vorgang kann ein paar Augenblicke dauern.

Die folgenden Parameter stehen zur Verfügung, wenn Sie die Policy-Verteilung in Active Directory konfigurieren:

- **Standardpfad der Domäne zur Speicherung von GPOs in:** Dies ist ein schreibgeschütztes Feld, das den Pfad angibt, in dem SafeGuard PortProtector-GPOs in Active Directory installiert werden. Policies werden als GPOs gespeichert, die später zu Benutzern und Computern zugewiesen werden, wie im Kapitel *Verteilen von Policies*, beschrieben. Dieses Feld gibt an, wo diese GPOs gespeichert und von wo sie während der Verteilung genommen werden.
- **Domäne bei jedem Veröffentlichen einer Policy auswählen (beim Speichern):** Wenn Sie einen Domänenwald haben, markieren Sie diese Option, damit Sie die Domäne auswählen können, an die die Policies beim Speichern veröffentlicht werden.
- **Zusammenführen von Policies aktivieren:** Wenn Sie dieses Kontrollkästchen aktivieren, werden auf Clients angewandte Policies mit denen zusammengeführt, die zuvor auf die Clients angewendet wurden. Auf diese Weise werden die geltenden Definitionen erzeugt. Eine Erläuterung finden Sie in *Zusammenführen von Policies* im Kapitel *Verteilen von Policies*.
  Wenn Sie dieses Kontrollkästchen später deaktivieren, wird die letzte Policy angewandt, und nur diese Policy wird nach der nächsten Aktualisierung in Kraft sein.

**Registry-Dateien in einem freigegebenen Ordner**

Aktivieren Sie die Option **Policies an freigegebenen Ordner veröffentlichen**, um anzugeben, dass SafeGuard PortProtector-Policies in einem freigegebenen Ordner im Format einer Registry-Datei gespeichert werden. Diese Dateien können dann mittels eines Drittanbieter-Tools an die Registry des Computers, auf dem SafeGuard PortProtector Client installiert ist, verteilt werden. Bei dieser Option wird Active Directory nicht verwendet.

Hinweis: Wenn Sie die zuvor beschriebene Option **Active Directory verwenden** genutzt haben und dann später diese Option wählen (und die Option Active Directory deaktivieren), werden alle vorhandenen Policies in den angegebenen, freigegebenen Ordner kopiert, und von diesem Zeitpunkt an werden alle Policies nur als Registry-Dateien in einem freigegebenen Ordner gehandhabt. Dieser Vorgang kann ein paar Augenblicke dauern.

**So geben Sie an, dass Policies als Registry-Dateien veröffentlicht werden:**

1 Markieren Sie **Policies an freigegebenen Ordner veröffentlichen**.

2 Geben Sie im Feld **Pfad zum Speichern von Policy-Registry-Dateien (.reg)** den freigegebenen Ordner ein, oder suchen Sie ihn, in dem diese Registry-Dateien gespeichert werden.

**Hinweis:** Wenn Sie eine Management Console benutzen, die sich nicht auf demselben Computer wie der Management Server befindet, ist der ausgewählte Pfad relativ zum Server, nicht zur Console.

3 Stellen Sie Folgendes sicher:

4 Auf den angegebenen Ordner kann von Ihrem Drittanbieter-Tool zugegriffen werden, um die Policies an SafeGuard PortProtector Clients zu verteilen.

5 Auf den angegebenen Ordner kann von dem Benutzerkonto, das Sie oben in *Server Domain Credentials* angegeben haben, zugegriffen werden (Lesen und Schreiben), so dass der Management Server die Policies an diesen Ordner veröffentlichen kann.

6 Optional – Sie können **Ausführbare Datei nach Veröffentlichung ausführen** aktivieren (siehe unten).

Wenn diese Option genutzt wird, erzeugt SafeGuard PortProtector zwei Kopien von der Registry-Datei, von denen eine für Computer (zum Beispiel **MyPolicy(MACHINE).reg**) und eine für Benutzer (zum Beispiel namens **MyPolicy(USER).reg**) geeignet ist.

Weitere Informationen finden Sie in *Kapitel 4, Verteilen von* Policies.

##### 7.4.1.1.1 Ausführbare Datei nach Veröffentlichung ausführen

Gegebenenfalls möchten Sie den Vorgang, bei dem Policies durch ein Drittanbieter-Tool verteilt werden (wie etwa SMS, Novell eDirectory), nach dem Bearbeiten/Erstellen von Policies automatisieren.

Diese Option ermöglicht die automatische Aktivierung einer ausführbaren Datei, wenn Policies als. reg-Dateien veröffentlicht werden. Diese ausführbare Datei führt dann die nötigen Funktionen aus, um dem Drittanbieter-Tool die Policy-Änderung mitzuteilen.

Für Informationen über APIs und Schnittstellenparameter wenden Sie sich bitte an den Sophos Support: mailto:support@sophos.com.

#### 7.4.1.2 Policy-Vorlage

Jedes Mal, wenn Sie eine neue Policy erstellen, werden Vorgabewerte für die Sicherheitsoptionen (Ports, Geräte etc.) und für die Einstellungen (Endbenutzer-Meldungen, Log-Intervalle etc.) angezeigt.

Mit dieser Option können Sie eine beliebige, bereits von Ihnen definierte Policy als Vorlage bestimmen, die bei der Erstellung neuer Policies die Standardpolicy ersetzt. Das ist vor allem dann nützlich, wenn Sie spezifische Einstellungen haben, die Sie als Ausgangsbasis anstelle der Standardeinstellungen bevorzugen.

So wählen Sie eine Policy als Vorlage aus:

Markieren Sie das Kontrollkästchen und wählen Sie die Policy aus der Dropdown-Liste aus.

**Hinweis:** Diese Option ist deaktiviert, bis Sie mindestens eine Policy erstellt haben.

#### 7.4.1.3 Abwärtskompatibilität

Wenn Sie Ihren SafeGuard PortProtector Management Server von einer früheren Version (3.1 oder niedriger) aufgerüstet haben, aber Ihre Clients noch nicht aufgerüstet haben, möchten Sie vielleicht, dass die von dieser Version veröffentlichten Policies mit den Clients der älteren Version kompatibel sind.

Nachdem alle SafeGuard PortProtector Clients in Ihrem Netz aufgerüstet wurden, empfehlen wir Ihnen, diese Option zu deaktivieren.

**So veröffentlichen Sie abwärtskompatible Policies:**

Markieren Sie das Kontrollkästchen im Abschnitt *Abwärtskompatibilität*. Ab diesem Zeitpunkt veröffentliche Policies sind mit früheren Client-Versionen kompatibel.

#### 7.4.1.4 Zulassen/Sperren nicht klassifizierter Geräte

Nicht klassifizierte Geräte können nicht von SafeGuard PortProtector in eine der in Anhang C – Unterstützte Gerätetypen aufgeführten Gerätekategorien eingeordnet werden.

SafeGuard PortProtector ist im Allgemeinen in der Lage, fast jedes Gerät zu klassifizieren. Einige Geräte passen jedoch in keine der integrierten Gerätekategorien oder verfügen nicht über den richtigen Mechanismus, der ihre Klassifizierung durch SafeGuard PortProtector oder das Betriebssystem selbst ermöglicht. Zu diesem Zweck bietet SafeGuard PortProtector eine spezielle Bearbeitungsmöglichkeit für nicht klassifizierte Geräte, wie in diesem Abschnitt beschrieben.

Normalerweise möchte eine Organisation nicht, dass unbekannte (nicht klassifizierte) Geräte über die eingeschränkten Ports an ihren Endpunkten angeschlossen werden, weil das eine Sicherheitsverletzung darstellen könnte.

Während der anfänglichen Einsatzphasen von SafeGuard PortProtector ist es jedoch möglich, das eine Organisation bei Bedarf den Zugriff von nicht klassifizierten Geräten zeitweilig zulassen möchte. Auf diese Weise wird ein reibungsloser Übergang zu einer sichereren Arbeitsweise ermöglicht, ohne nicht klassifizierte Geräte verfrüht zu sperren, bevor Sie in eine Policy übernommen werden können, von der sie explizit zugelassen werden.

Daher möchte eine Organisation unter Umständen anfangs **zulassen**, dass nicht klassifizierte Geräte weiterhin auf die Ports der Organisation zugreifen, wobei jeder Zugriff protokolliert wird. Der Administrator kann dann die die SafeGuard PortProtector-Logs abfragen und erkennen, welche nicht klassifizierten Geräte benutzt werden, um dann diese spezifischen Geräte in einer Policy zuzulassen.

Nachdem dieser berechtigende Ansatz während der Anfangsphase genutzt wurde, und nachdem der Administrator die freizugebenden nicht klassifizierten Geräte in einer oder mehreren Policies definiert hat, wird empfohlen, nicht klassifizierte Geräte zu sperren.

**Hinweis:** Die Einstellung nicht klassifizierter Geräte als **Zugelassen** beeinflusst die Art und Weise, in der Policies zusammengeführt werden, so dass die Gerätekontrolldefinitionen mit den meisten Einschränkungen aller für dieselbe Organisationseinheit geltenden Policies wirksam werden. Weitere Informationen hierzu finden Sie in *Zusammenführen von Policies bei nicht klassifizierten,*
*zugelassenen Geräten*.

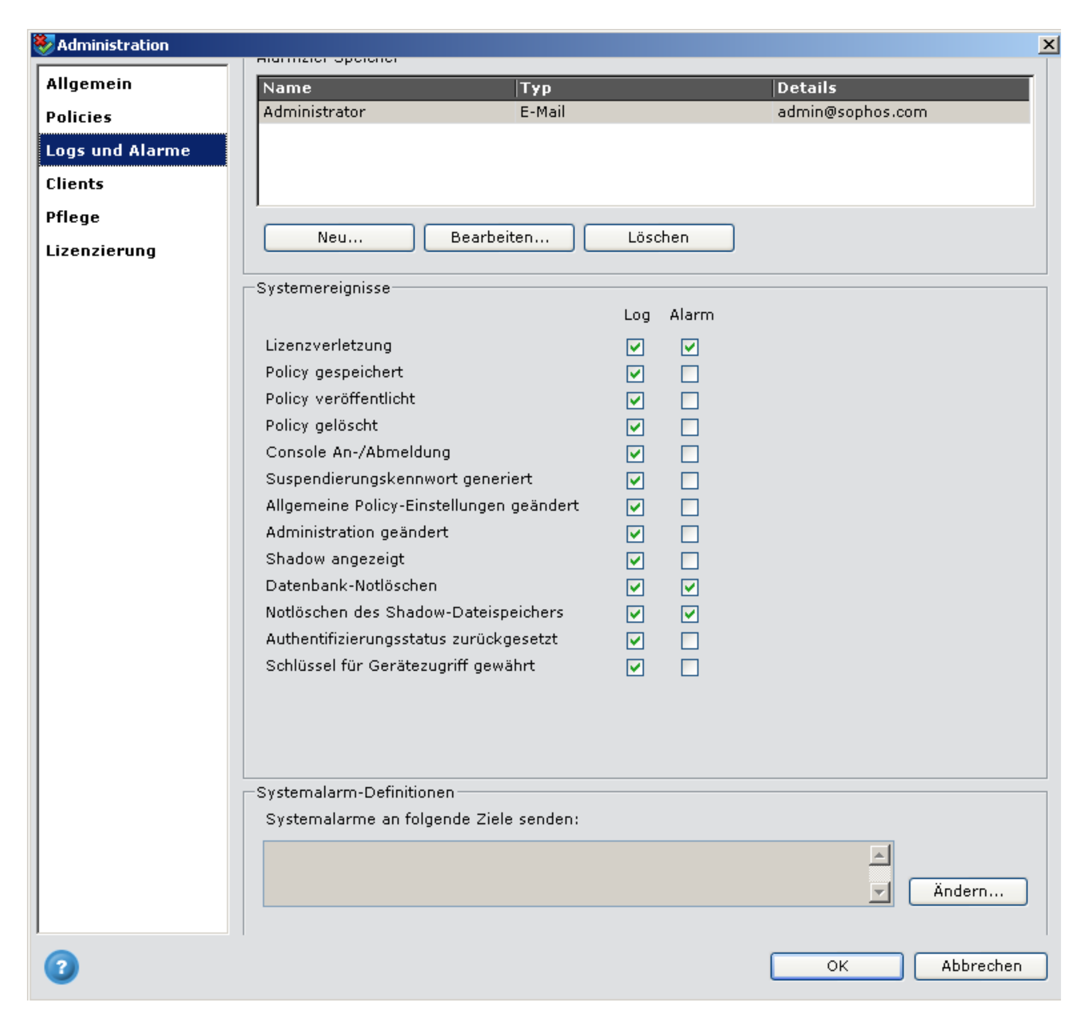
**Hinweis:** Wenn nicht klassifizierte Geräte als **Zugelassen** auf der Seite *Policies* im Fenster *Administration* definiert werden, wird dadurch das Fenster *Gerätekontrolle* auf der Registerkarte *Allgemein* des Fensters *Policy* beeinflusst. Das Fenster *Gerätekontrolle* zeigt **Zulassen** ( ) im Bereich **Devices Not Approved in Device Types or White List** für *Nicht klassifizierte Geräte* unten im Fenster. Dadurch wird gekennzeichnet, dass nicht klassifizierte Geräte zugelassen werden, und dass die Gerätekontrolle der Policy-Zusammenführung beeinflusst wurde.

**So definieren Sie die Sicherheitsaktionen für nicht klassifizierte Geräte:**

Wählen Sie im *Abschnitt Sicherheitsmaßnahme für nicht klassifizierte Geräte* entweder die Option **Nicht klassifizierte Geräte sperren (empfohlen)** oder die Option **Nicht klassifizierte Geräte zulassen**, wie oben beschrieben.

## 7.5 Konfigurieren der Einstellungen auf der Registerkarte Logs und Alarme

Log- und Alarmdefinitionen sowie Ausgabeziele werden auf der Registerkarte *Logs und Alarme* des Fensters *Administration* definiert:



## 7.5.1 Log- and Alarmeinstellungen

Auf der Registerkarte *Logs und Alarme* können Sie das Alarmziel Speicher sowie Log- und Alarmdefinitionen und Alarmziele für Management Server-Ereignisse konfigurieren. Sie enthält die folgenden Abschnitte:

- *Alarmziel Speicher*
- *System*
- *Systemalarm-Definitionen*

**Hinweis:** Bei jeder Änderung einer der Einstellungen auf dieser Registerkarte müssen Sie unten im Fenster **Administration** auf *OK* klicken, damit die Änderungen übernommen werden.

### 7.5.1.1 Alarmziel Speicher

Hier können Sie die in Ihrem Netzwerk zum Versenden von Alarmen verfügbaren Ziele ansehen, bearbeiten, definieren und löschen. Unter einem Ziel versteht man die Adresse, an die Alarme gesendet werden.

Die Liste dieser Adressen wird als *Alarmziel Speicher* bezeichnet. Nachdem Sie das Repository angelegt haben, können Sie daraus die gewünschten Ziele für Systemalarme (siehe *Systemalarmdefinitionen*), für policy-spezifische Alarmeinstellungen (siehe *Definieren der Alarmeinstellungen* im Kapitel *Definieren von Policies*) und für globale Policy-Alarmeinstellungen (siehe *Schritt 9: Allgemeine Policy-Einstellungen definieren* im Kapitel *Definieren von Policies*) auswählen.

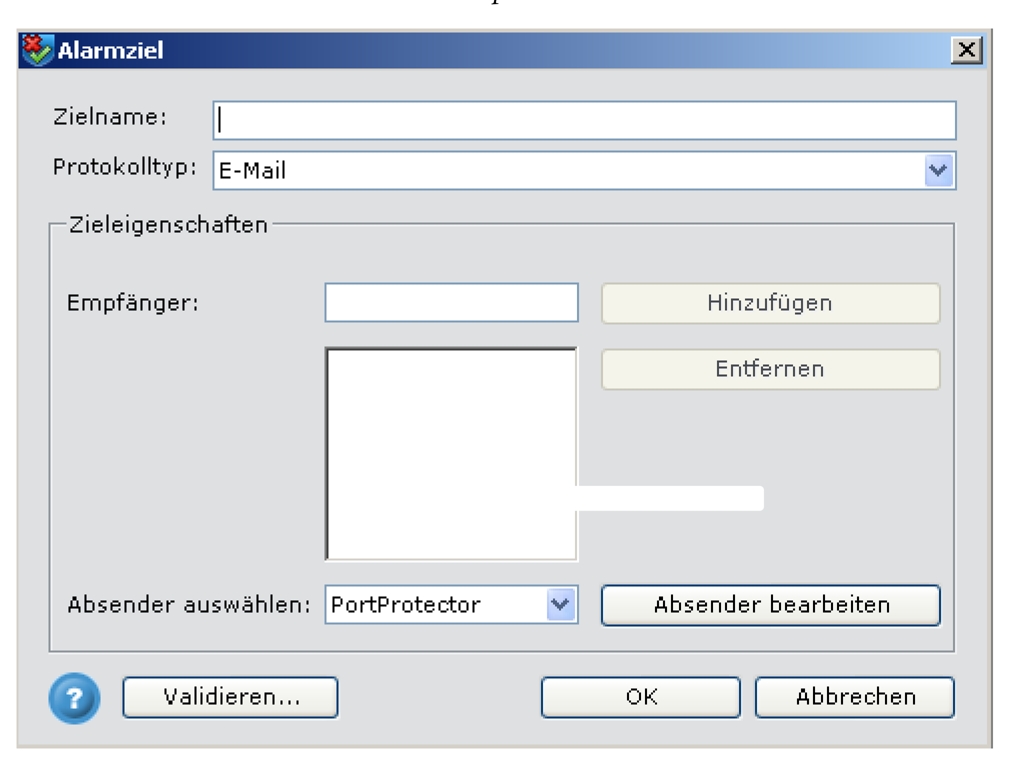
Die Ziele können zu mehrere Protokolltypen gehören, darunter:

- **E-Mail** – Senden an eine/mehrere Adressen
- **Windows Event Log** – Einfügen eines Logeintrag in ein bestimmtes Computer-Eventlog
- **SNMP** – Erzeugen eines SNMP-Trap, der an Netzwerküberwachungssysteme gesendet wird (d. h. HP Openview, IBM Tivolli)
- **Executable** – Ausführen einer ausführbaren Datei, die anhand der Alarminformation eine beliebige Aktion ausführt
- **Syslog** – Senden einer Nachricht an einen Syslog-kompatiblen Server.

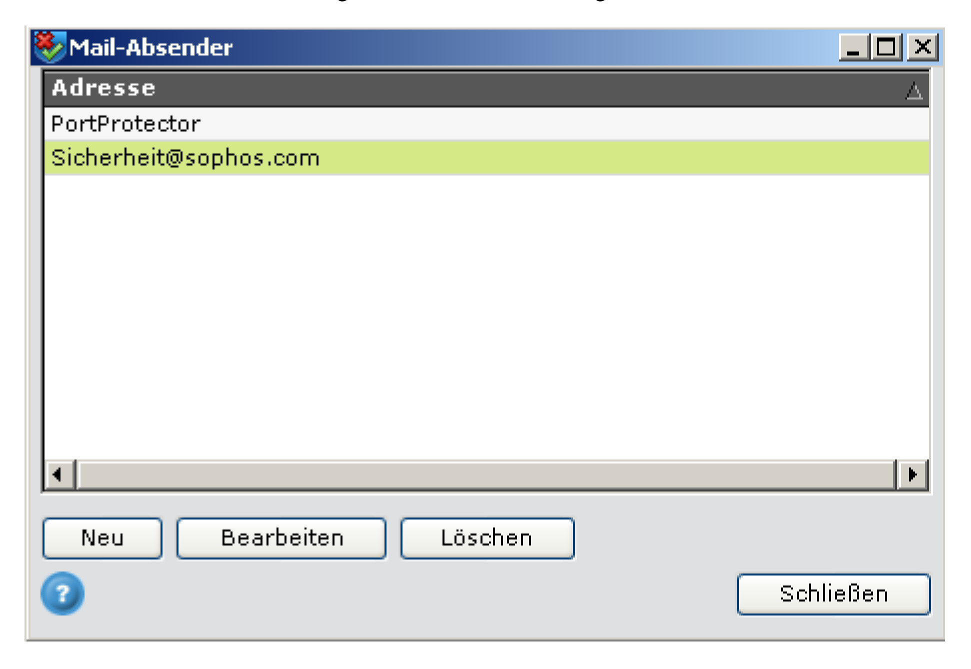
Alarmdefinitionen werden im Fenster *Alarmziel* festgelegt.

**So öffnen Sie das Fenster *Alarmziel*:**

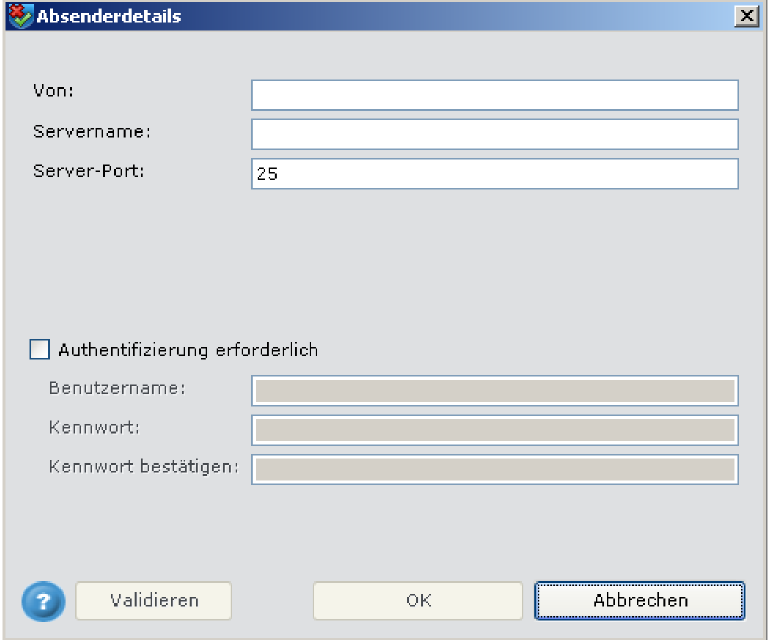
1 Klicken Sie im Abschnitt *Alarmziel Speicher* auf **Neu**. Das Fenster *Alarmziel* erscheint:




2 Um ein neues Versenden zu definieren, klicken Sie auf die Schaltfläche **Absender bearbeiten**, um das folgende Fenster anzuzeigen:



Sie können auf die Schaltfläche **Neu** klicken, um im folgenden Fenster einen neuen Absender hinzuzufügen.




### 7.5.1.2 Definieren eines neuen E-Mail-Absenders

Im Folgenden sind die erforderlichen Eigenschaften für die Festlegung eines neuen E-Mail-Absenders aufgeführt:

- **Von** – Dieses Feld erscheint im Feld **From** der gesendeten E-Mails.
- **Servername** – Der Hostname Ihres E-Mail-Ausgangsservers (SMTP). Sie können auch eine IP-Adresse angeben.
- **Server-Port** – Der TCP-Port: für das Versenden von E-Mails. Normalerweise ist dies Port 25. Wenn Sie ein sicheres E-Mail-System verwenden, kann der Port ein anderer sein.
- **Authentifizierung** (**optional**) – Wenn Ihre E-Mail-Ausgangsserver eine Authentifizierung verlangt, füllen Sie auch die folgenden Felder aus:
  - **Benutzername**
  - **Kennwort**

#### 7.5.1.3 Festlegen eines Alarmziels

Im Folgenden sind die erforderlichen Eigenschaften für die einzelnen Protokolltypen aufgeführt:

- **E-Mail**
    - **Empfänger –** Geben Sie eine gültige E-Mail-Adresse ein, an die die E-Mail gesendet wird. Sie können auch mehrere Adressen, durch Komma/Semikolon getrennt, eingeben. Wählen Sie **Hinzufügen**. um die eingegebene Mail-Adresse zur Empfängerliste hinzuzufügen.
    - Wählen Sie im Feld **Absender wählen** die E-Mail-Adresse aus der Dropdown-Liste, die als Absender angegeben werden soll. Die Dropdown-Liste zeigt die Absender, die vorher in SafeGuard PortProtector entweder in diesem Fenster oder im Fenster *Report planen* eingegeben wurden. Sie können auch auf die Schaltfläche **Absender bearbeiten** klicken, um einen neuen Absender zu definieren, einen vorhandenen Absender zu bearbeiten oder einen Absender zu löschen.

**Hinweis:** Die Dropdown-Liste im Fenster *Alarmziel* zeigt die Absender, die vorher in SafeGuard PortProtector in diesem Fenster eingegeben wurden.

- **SNMP**
    - **Servername –** Der Hostname Ihres SNMP-Servers. Sie können auch eine IP-Adresse angeben.
    - **Server-Port –** Der TCP-Port: für das Versenden von SNMP-Traps. Normalerweise ist dies Port 162.
- **Windows Event Log**
    - **Host-Name –** Der Name des Hosts, auf den die Windows-Ereignisprotokolle geschrieben werden. Sie können auch eine IP-Adresse angeben.
- **Ausführbare Datei**
    - **Pfad zu ausführbarer Datei–** Der Pfad zu einer ausführbaren Datei, die ggf. durch einen Alarm gestartet werden kann.

Für weitere Informationen über API-Parameter wenden Sie sich bitte an den Sophos Support: mailto:support@sophos.com.

**So fügen Sie ein Alarmziel hinzu:**

1 Geben Sie in diesem Fenster die erforderlichen Details ein, und klicken Sie auf **OK**.

2 Nachdem Sie auf **OK** geklickt haben, überprüft das System das von Ihnen eingegebene Ziel. Falls es nicht gültig ist, prüfen Sie Ihre Einstellungen und versuchen Sie es noch einmal.

3 Sie können auch auf **Validieren** klicken, um die Validierung manuell durchzuführen.

Nachdem Sie den Alarmziel Speicher, können Sie daraus die gewünschten Ziele für Systemalarme (siehe *Systemalarmdefinitionen*), für policy-spezifische Alarmeinstellungen (siehe *Definieren der Alarmzieleinstellungen* im Kapitel *Definieren von Policies*) und für globale Policy-Alarmeinstellungen (siehe *Schritt 9: Allgemeine Policy-Einstellungen definieren* im Kapitel *Definieren von Policies*) auswählen.

**Hinweis:** Wenn Sie die Eigenschaften eines Ziels ändern, betrifft das alle Alarme, die dieses Ziel nutzen – Systemalarme, policy-spezifische Alarme und globale Policy-Alarmeinstellungen.

### 7.5.2 Systemereignisse

Systemereignisse verfolgen sowohl vom Management Server generierte Ereignisse als auch auf den Management Consoles ausgeführte Aktionen. In diesem Abschnitt definieren Sie, welche Ereignisse protokolliert werden (und in Server-Logs angezeigt werden können) und welche auch eine Alarm erzeugen.

Zu den Systemereignissen gehören:

- Lizenzverletzung
- Policy gespeichert
- Policy veröffentlich
- Policy gelöscht
- Consolen-An-/Abmeldung
- Suspendierungskennwort generiert
- Global Policy Changed
- Serverkonfiguration geändert
- Schlüssel für Zurücksetzen der Festplattenverschlüsselung gewährt
- Schlüssel für Wiederherstellung der Festplattenverschlüsselung gewährt
- Schlüssel für einmaligen Zugriff für Festplattenverschlüsselung gewährt
- Shadow angezeigt
- Geplanter Report ist fehlgeschlagen
- Datenbank-Notlöschen
- Notlöschen des Shadow-Dateispeichers

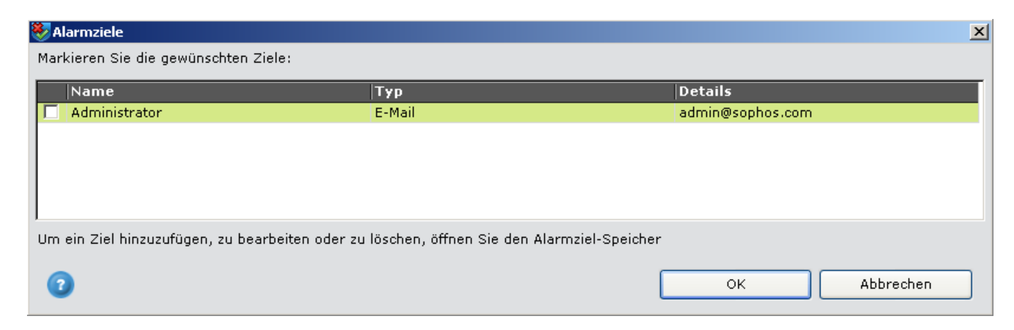
Gemäß Voreinstellung werden alle Ereignisse protokolliert. Sie können einige der Logs deaktivieren oder Ereignisse bestimmen, für die der Management Server auch einen Alarm senden soll.

#### 7.5.2.1 Systemalarmdefinitionen

Wählen Sie hier die Ziele, an die der Management Server die aufgrund von Systemereignissen generierten Alarme senden soll. Alarme werden nur für die Ereignistypen versendet, die Sie im vorigen Abschnitt ausgewählt haben.

**So fügen Sie Ziele hinzu bzw. entfernen sie:**

1 Klicken Sie auf **Ändern**. Das Fenster *Alarmziele* wird angezeigt, in dem alle verfügbaren Alarmziele aufgelistet werden, die zuvor unter Alarmziel Speicher definiert wurden (siehe *Alarmziel Speicher* in *Kapitel 8, Administration.*).

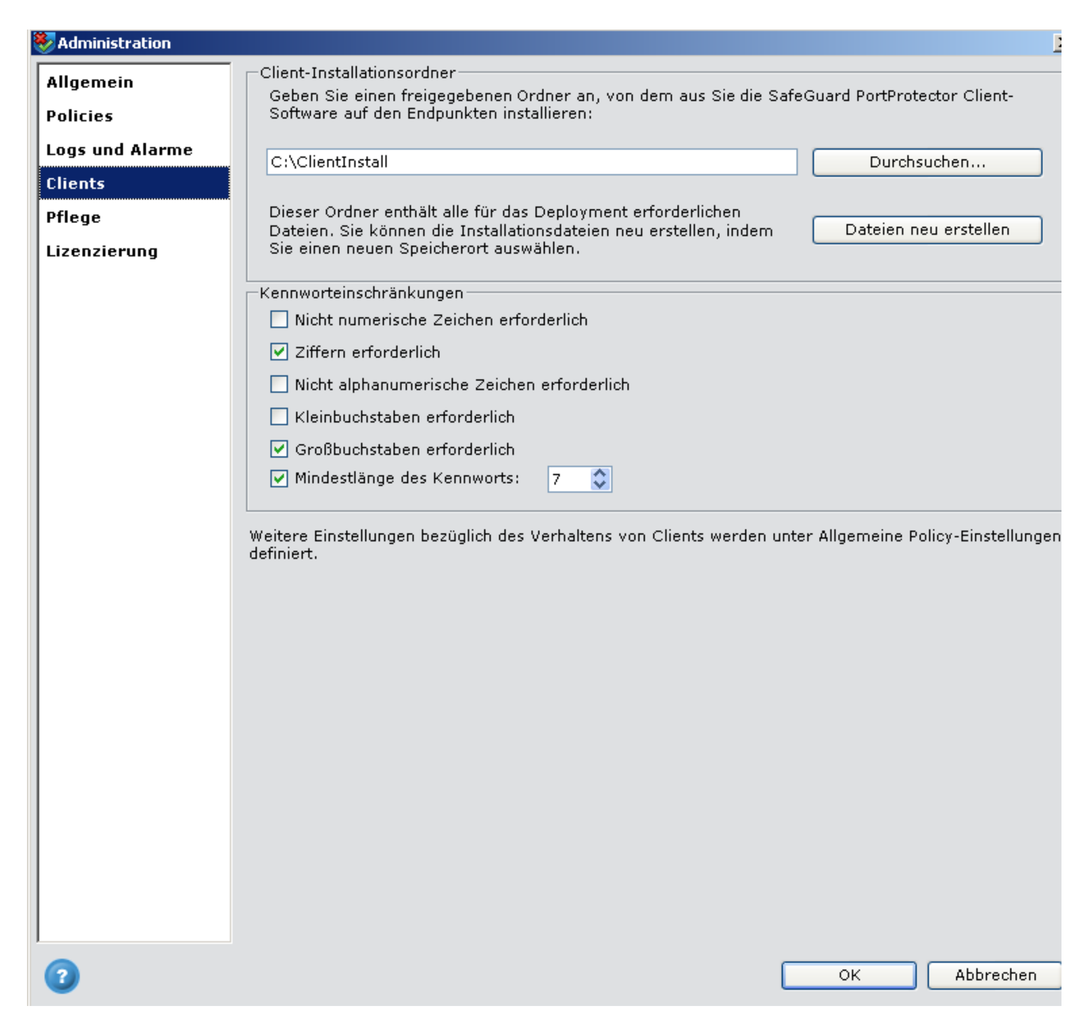



2 Aktivieren bzw. deaktivieren Sie die Ziele wie gewünscht, und klicken Sie auf **OK**.

**Hinweis:** Informationen zum Hinzufügen, Bearbeiten und Löschen eines Ziels finden Sie in *Alarmziel Speicher* in *Kapitel 8, Administration*.

## 7.6 Konfigurieren der Einstellungen auf der Registerkarte Clients

Client-Administrationseinstellungen werden auf der Registerkarte *Clients* des Fensters *Administration* definiert:




### 7.6.1 Client-Einstellungen

Auf der Registerkarte *Clients* können Sie im Abschnitt Client-Installationsordner den Ordner konfigurieren, in dem die Client-Installationsdateien gespeichert werden sollen, und im Abschnitt *Kennworteinschränkungen* die Kriterien für die Verwendung von Kennwörtern in SafeGuard PortProtector definieren.

**Hinweis:** Weitere Client-Einstellungen, wie etwa Kennwort für die Deinstallation, Log-Intervall und Sichtbarkeitseinstellungen für den Client, werden im Fenster *Allgemeine Policy-Einstellungen* festgelegt, das Sie über das Menü *Extras* erreichen und das in *Schritt 9: Allgemeine Policy-Einstellungen definieren* im Kapitel *Definieren von Policies*, beschrieben ist.

#### 7.6.1.1 Client-Installationsordner

Hierbei handelt es sich um den Ordner, in den der Management Server die für die Installation von SafeGuard PortProtector Clients auf den Endpunkten erforderlichen Dateien exportiert. Um Clients zu installieren, müssen Sie einen Ordner definieren, in dem die Installationsdateien angelegt werden.

Dieser Ordner sollte normalerweise ein Netzwerkpfad sein, der für die Installation der Software auf den Endpunkten zugänglich ist.

**Hinweis:** Bei jeder Änderung einer der Einstellungen auf dieser Registerkarte müssen Sie unten im Fenster *Administration* auf **OK** klicken, damit die Änderungen übernommen werden.

**So legen Sie den freigegebenen Ordner für Client-Installationsdateien fest:**

1 Klicken Sie auf **Durchsuchen**.

2 Wählen Sie einen Netzwerkpfad für den freigegebenen Ordner, und klicken Sie auf **OK**.

3 Sobald Sie einen neuen Pfad festgelegt haben, kopiert der Server die folgenden Dateien in den neuen Pfad:

- SafeGuardPortProtectorClient.msi
- SafeGuardPortProtectorClient.exe
- ClientConfig.scc

4 Sie können auch jederzeit auf **Dateien neu erstellen** klicken, um die Dateien neu zu erstellen, falls sie aus irgendeinem Grund beschädigt wurden.

Anweisungen zum Client-Deployment finden Sie im SafeGuard PortProtector Installationshandbuch.

**Hinweis:** Weitere Client-Einstellungen, wie etwa Kennwort für die Deinstallation, Log-Intervall und Sichtbarkeitseinstellungen für den Client, werden im Fenster *Allgemeine Policy-Einstellungen* festgelegt, das Sie über das Menü *Extras* erreichen und das in *Schritt 9: Allgemeine Policy-Einstellungen definieren* im Kapitel *Definieren von Policies* beschrieben ist.

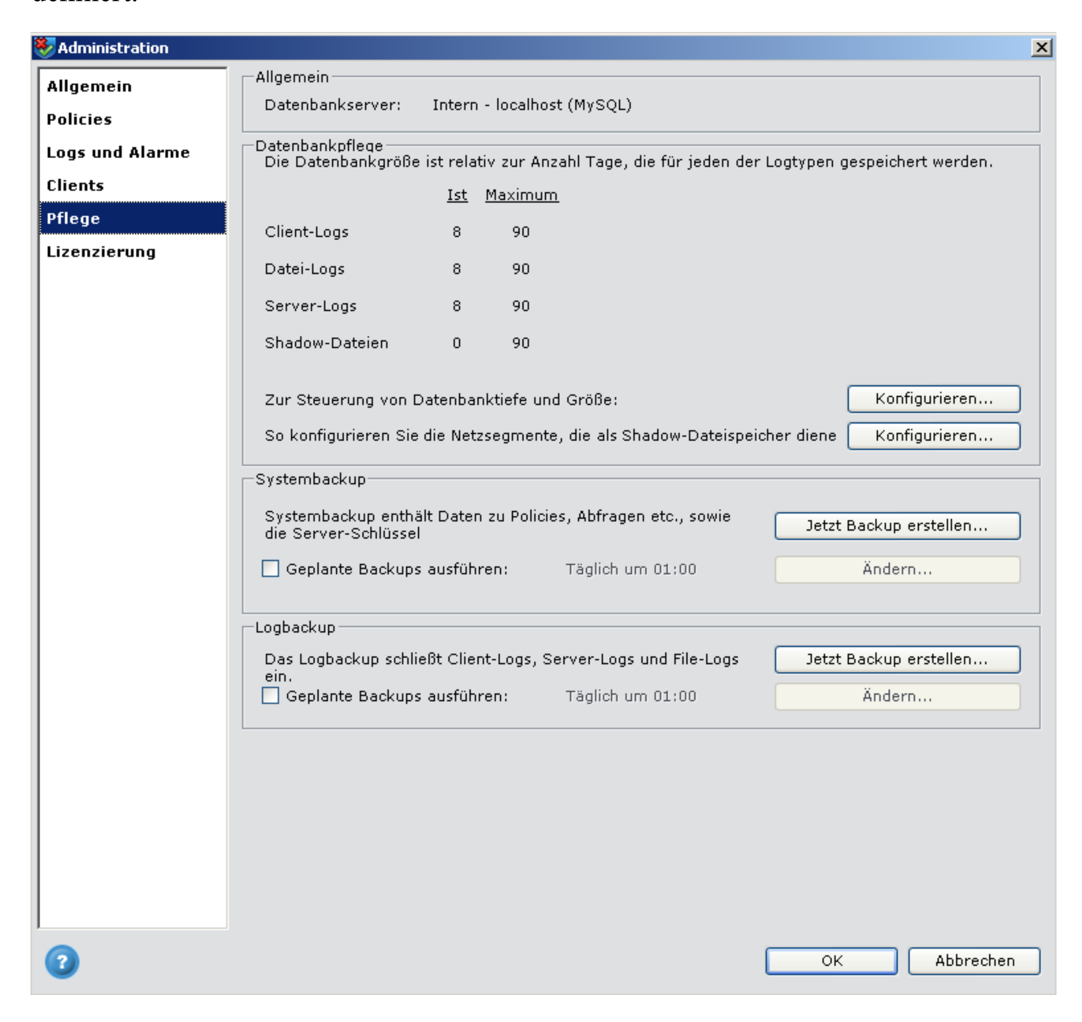
#### 7.6.1.2 Kennworteinschränkungen

In SafeGuard PortProtector gibt es einige Stellen, an denen die Bedienung kennwortgeschützt ist, wie etwa beim Deinstallieren eines Clients, beim Einsatz des Offline Access Utility, beim Zugriff auf die Administration und auf einem SafeGuard PortProtector Client,

Markieren Sie die gewünschten Optionen in diesem Bereich, um die Eigenschaften der Kennwörter zu steuern, die in SafeGuard PortProtector genutzt werden können, wie etwa Art und Anzahl der Zeichen sowie maximale Kennwortlänge,. Sie können eine beliebige Kombination der in diesem Abschnitt des Fensters verfügbaren Optionen wählen.

## 7.7 Konfigurieren der Einstellungen auf der Registerkarte Pflege

Systempflegeeinstellungen werden auf der Registerkarte *Pflege* des Fensters *Administration* definiert:



## 7.7.1 Systempflegeeinstellungen

Auf der Registerkarte *Maintenance* können Sie verschiedene Aktivitäten der Systempflege durchführen. Sie können hier Einstellungen für Datenbankpflege und den System-Backup definieren. Sie enthält die folgenden Abschnitte:

- *Allgemein*
- *Datenbankpflege*
- *System Backup*
- *Log Backup*

**Hinweis:** Bei jeder Änderung einer der Einstellungen auf dieser Registerkarte müssen Sie unten im Fenster *Administration* auf **OK** klicken, damit die Änderungen übernommen werden.

### 7.7.1.1 Allgemein

Dieser Abschnitt zeigt den Namen des Datenbankservers, und ob es sich um den internen MySQL-Server von SafeGuard PortProtector oder einen externen MS SQL-Server handelt.

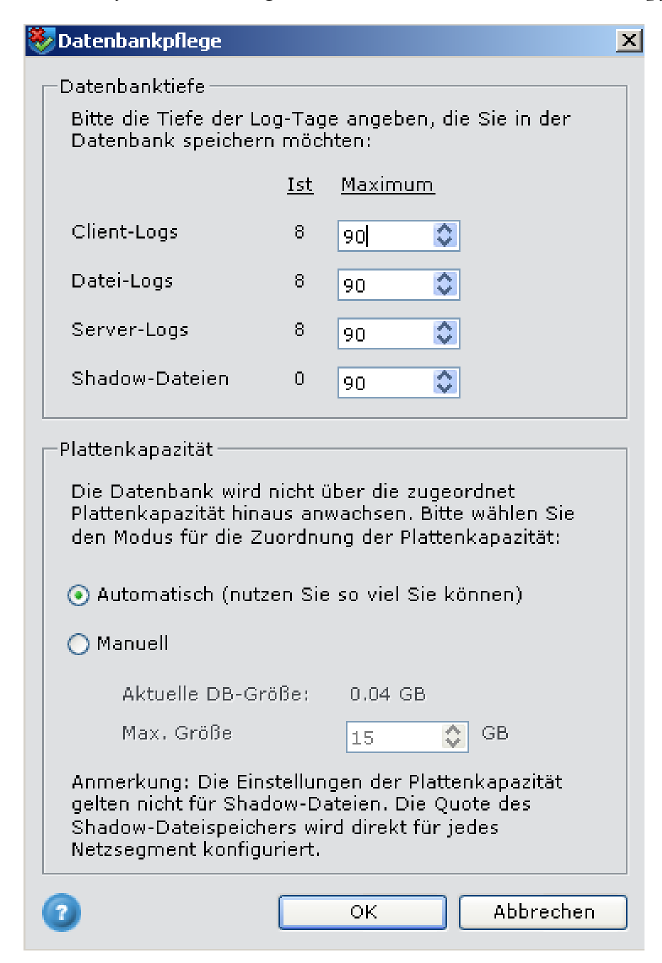
### 7.7.1.2 Datenbankpflege

Dieser Abschnitt befasst sich mit der Verwaltung der Datenbank. Hier legen Sie die Anzahl der Protokollierungstage (Tiefe) fest, die Sie für jeden Logtyp speichern möchten, und definieren die der Datenbank zugeteilte Plattenkapazität, bei der Logs den größten Teil der Plattenkapazität ausmachen. Über die Datenbankverwaltung können Sie die benötigte Tiefe – oder zumindest eine Tiefe soweit wie möglich – speichern. Dies definieren Sie im Fenster *Datenbankpflege* (siehe auch Definieren der Datenbankpflege-Einstellungen).

Darüber hinaus können Sie in diesem Abschnitt den Netzanteil definieren, der als zentraler Speicher für Shadow-Dateien genutzt werden soll, wie im Abschnitt *Definieren der Netzanteile für Datei-Shadowing* beschrieben.

**So öffnen Sie das Fenster *Datenbankpflege*:**

Klicken Sie im Abschnitt *Datenbankpflege*, neben dem Feld *Zur Steuerung von Datenbanktiefe und Größe* auf **Konfigurieren**. Das Fenster *Datenbankpflege* wird angezeigt:




#### 7.7.1.2.1 Definieren der Datenbankpflege-Einstellungen

Das Fenster *Datenbankpflege* enthält zwei Abschnitte:

- **Datenbanktiefe:** Zeigt die tatsächlich Anzahl an Tagen, die derzeit für jeden Logtyp gespeichert wird, und ermöglicht es Ihnen, die erforderliche (maximale) Anzahl der Speichertage pro Logtyp festzulegen.
- **Plattenkapazität:** Hier können Sie die Plattenkapazität für die Datenbank automatisch oder manuell zuteilen. Standardmäßig wird die Plattenkapazität automatisch verwaltet und soll Ihnen die gewünschte Tiefe ermöglichen. Wir empfehlen, dass Sie die Plattenkapazität nur dann manuell zuteilen, wenn auf demselben Server eine andere Anwendung läuft, die schnell zunehmend viel Speicherkapazität nutzt.

**Hinweis:** Wenn Sie eine externe Datenbank einsetzen, wird dieser Abschnitt nicht angezeigt, weil in diesem Fall die Plattenkapazität nicht von SafeGuard PortProtector verwaltet wird.

**So konfigurieren Sie die Datenbankpflege-Einstellungen:**

1 Legen Sie im Abschnitt *Datenbanktiefe* die Anzahl der Speichertage für jeden Logtyp – Client-Logs, File-Logs, Server-Logs und Shadow-Dateien – fest.

2 Klicken Sie auf die entsprechende Optionsschaltfläche im Abschnitt *Plattenkapazität*, um anzugeben, ob die Zuordnung der Plattenkapazität automatisch erfolgen soll, oder ob Sie sie manuell zuordnen möchten (die aktuelle Datenbankgröße wird angezeigt).

**Hinweis:** Wenn Sie eine externe Datenbank einsetzen, wird dieser Abschnitt nicht angezeigt, weil in diesem Fall die Plattenkapazität nicht von SafeGuard PortProtector verwaltet wird.

3 Wenn Sie die manuelle Zuordnung der Plattenkapazität wählen, legen Sie die maximal von der Datenbank zu nutzende Plattenkapazität fest.

4 Klicken Sie auf **OK**. Log-Tiefe: und Datenbankgröße entsprechen jetzt diesen Einstellungen.

**Hinweis:** Wenn Sie die interne Datenbank von SafeGuard PortProtector benutzen und die Plattenkapazität für die gewünschte Datenbanktiefe zu gering ist, wird ein Notlöschen durchgeführt, bei dem die ältesten Datensätze gelöscht werden, um Platz zu schaffen. Falls dies geschieht, wird im Fenster *Datenbankpflege* und in Abschnitt *Datenbank* in der Home-Welt eine Nachricht angezeigt. Hiermit werden Sie informiert, dass die Datenbank derzeit wegen geringer Plattenkapazität nicht die erforderlichen Tage an Tiefe enthält und Sie weitere Plattenkapazität zuordnen oder die Tiefenanforderungen ändern sollten.

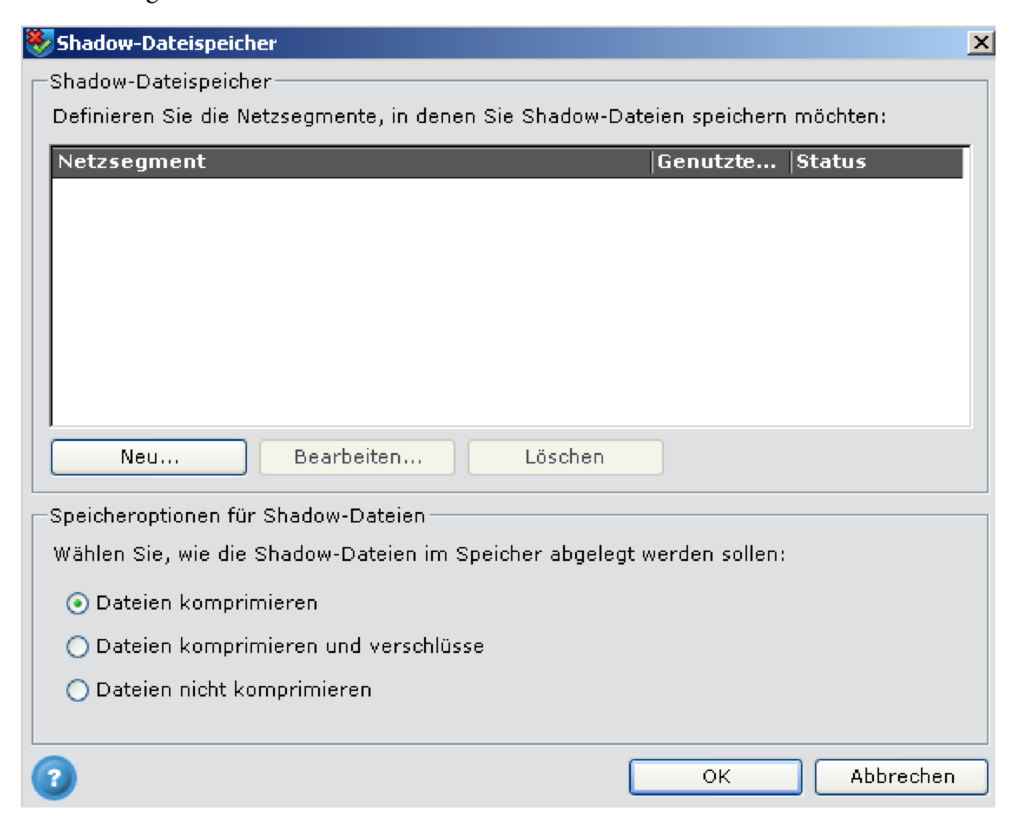
### 7.7.1.3 Definieren der Netzanteile für Datei-Shadowing

Dieser Abschnitt beschreibt, wie Sie den Netzanteil definieren, der als zentraler Speicher für Shadow-Dateien genutzt werden soll. Ein Administrator kann ein oder mehrere Netzsegmente als zentralen Speicher für das File-Shadowing definieren. Wenn mehrere Netzsegmente definierte werden, wird ein Lastausgleichsalgorithmus genutzt, um sicherzustellen, dass die Last auf alle Teile gleichmäßig verteilt wird.

Hinweis: Ähnlich wie bei der Protokollierung werden Shadow-Dateien lokal auf dem geschützten Computer gespeichert, bis sie auf einen Server geleitet werden. Weitere Informationen hierzu finden Sie in *Definieren der Einstellungen für Datei-Shadowing*.

**So konfigurieren Sie die Netzanteile für das File-Shadowing:**

1 Klicken Sie im Bereich **Datenbankpflege** rechts neben dem Feld **So konfigurieren Sie die Netzsegmente, die als Shadow-Dateispeicher dienen** auf **Konfigurieren.** Das folgende Fenster wird angezeigt, das die bereits als Speicher für Shadow-Dateien definierten Netzsegmente aufführt.




2 Klicken Sie auf die Schaltfläche **Neu**, um einen neuen Netzanteil zu definieren. Das folgende Fenster wird angezeigt:




3 Klicken Sie auf **Durchsuchen**, um ein Fenster zu öffnen, in dem Sie den Pfad zu diesem Netzsegment angeben können.

4 Wählen Sie den Pfad aus, und klicken Sie dann auf **Neuen Ordner erstellen**. Es wird ein Fenster angezeigt, in dem die Credentials (d. h. Anmeldeinformationen) für den Zugriff auf diesen Ordner angefordert werden.

5 Geben Sie die Credentials ein und klicken Sie auf **Validieren**, um den Zugriff auf den Ordner zu testen. Klicken Sie auf **OK**.

**Hinweis:** Wenn mehrere Netzsegmente definierte werden, wird ein Lastausgleichsalgorithmus genutzt, um sicherzustellen, dass die Last auf alle Teile gleichmäßig verteilt wird und dass im Fall einer Störung beim Zugriff auf einen der Anteile ein reibungsloser Fallover möglich ist.

6 Sie können die Dateien im Speicher komprimieren und verschlüsseln, indem Sie eine der folgenden Optionen wählen. Nur autorisierte Administratoren können auf verschlüsselte Dateien auf der Management Console zugreifen.

- *Dateien komprimieren*
- *Dateien komprimieren und verschlüsseln*
- *Dateien nicht komprimieren*

7 Der hinzugefügte Netzanteile wird standardmäßig im *Shadow-Dateispeicher* als Aktiv definiert. Sie können mit der rechten Maustaste darauf klicken, um die Option **Deaktivieren** zu wählen. Die Deaktivierung eines Netzanteils bedeutet, dass keine Shadow-Dateien mehr dorthin geschrieben werden. Jedoch können Dateien, die sich bereits in dem Netzanteil befinden, weiterhin von einem autorisierten Administrator betrachtet werden.
Sie können ein Netzsegment löschen, indem Sie ihn unter *Shadow-Dateispeicher* auswählen und auf **Löschen** klicken. Wenn Sie einen Netzanteil löschen, können **seine Dateien** nicht mehr von einem autorisierten Administrator betrachtet werden.

### 7.7.1.4 Systembackup

Es wird außerdem empfohlen, ein Backup Ihrer Konfiguration zu erstellen, so dass die vorhandene Konfiguration bei Bedarf wiederhergestellt werden kann, falls Sie den Management Server neu installieren müssen. Das Konfigurationsbackup schließt die Sicherung Ihrer Policy-Definitionen, Logabfragedefinitionen und Administrationseinstellungen ein. Sie können jederzeit ein Ad-hoc-Backup durchführen oder vordefinierte Backups planen.

**So führen Sie ein geplantes Backup aus:**

Markieren Sie im Abschnitt *Systembackup* das Kontrollkästchen **Geplante Backups ausführen**. Das Konfigurationsbackup wird zu den geplanten Zeiten ausgeführt (die nächste geplante Zeit wird angezeigt).

Sie können den Plan für das Systembackup ändern. Siehe *Planen des Systembackups*.

#### 7.7.1.4.1 Backup des Systems

Um ein Backup des Systems zu erstellen, müssen Sie ein Kennwort für die Backupdatei festlegen. Dieses Kennwort wird benötigt, wenn Sie dieses Backup zur Wiederherstellung Ihres Management Servers nutzen.

So erstellen Sie ein Backup des Systems:

1 Klicken Sie auf **Jetzt Backup erstellen.** Das Dialogfeld Systembackup wird angezeigt.




2 Wählen Sie einen Pfad, in dem die Backupdatei der Systemkonfiguration gespeichert werden soll.

3 Legen Sie ein Kennwort für die Backup-Datei fest und bestätigen Sie es.

4 Klicken Sie auf **OK**. Die Backupdatei der Systemkonfiguration ist gespeichert.

**Hinweis:**

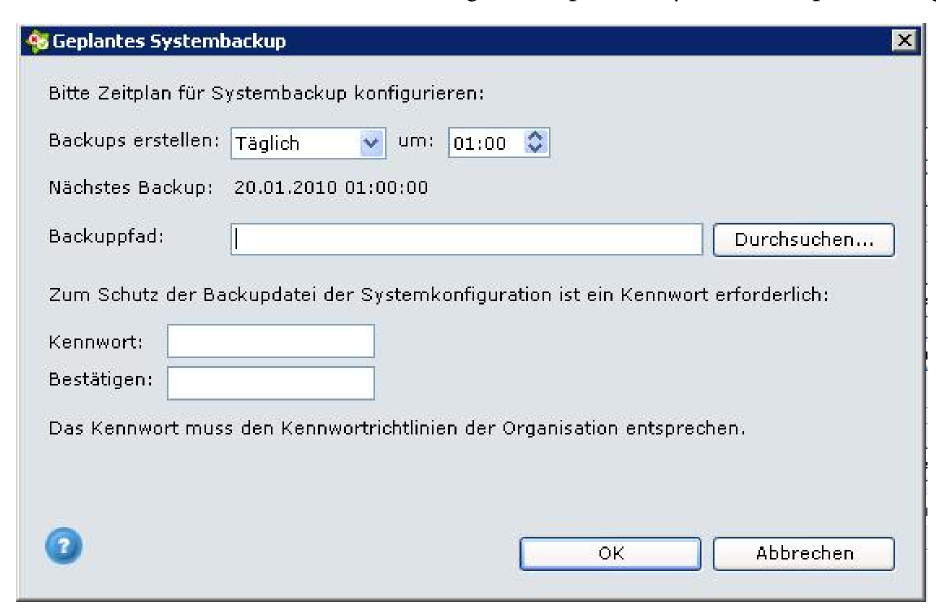
1. Sie können jederzeit ein Backup des Systems erstellen. Es wird empfohlen, mehrere Backups auf unterschiedlichen Computern und Standorten zu speichern.
2. Wenn Sie das Kennwort vergessen haben, erstellen Sie einfach ein neues Backup und benutzen Sie ein neues Kennwort.

#### 7.7.1.4.2 Planen des Systembackups

Sie können den Zeitplan für das Systembackup konfigurieren.

**Konfigurieren des Zeitplans für das Systembackup:**

1 Klicken Sie auf **Ändern.** Das Dialogfeld 'Geplantes Systembackup' wird angezeigt.




2 Legen Sie das Intervall für **Backups erstellen** (*Täglich*, *Wöchentlich*, *Monatlich*) und die Zeit fest.

3 Klicken Sie auf **Durchsuchen**, um den Pfad für das Backup auszuwählen.

4 Geben Sie ein Kennwort ein und bestätigen Sie es.

5 Klicken Sie auf **OK**. Der Zeitplan für das Systembackup ist jetzt festgelegt. Die Dateien des Systembackups werden gemäß den folgenden Namenskonventionen gespeichert: SystemBackup01JAN2009_2359.SCB, wobei 01Jan2009_2359 Datum und Zeit repräsentieren. Die aktuelle Datei wird nicht von der neuen Backupdatei überschrieben, so dass immer zwei Backupdateien vorhanden sind.

### 7.7.1.5 Log Backup

**Hinweis:** Wenn Sie eine externe Datenbank einsetzen, wird dieser Abschnitt nicht angezeigt, weil in diesem Fall die Sicherung nicht von SafeGuard PortProtector verwaltet wird.

Ähnlich wie die Konfiguration können Sie auch Ihre Logs sichern. Dazu gehören Client-Logs, Server-Logs und File-Logs. Sie können jederzeit ein Ad-hoc-Backup durchführen oder vordefinierte Backups planen.

**So führen Sie jederzeit ein Backup aus:**

1 Klicken Sie im Abschnitt *Logbackup* auf **Jetzt Backup erstellen.** Das Fenster *Logbackupdatei auswählen* wird geöffnet.

2 Wählen Sie den gewünschten Pfad und Dateinamen, und klicken Sie auf **Speichern.** Die Logs werden gesichert.

Sie können auch geplante Logbackups in regelmäßigen, vordefinierten Intervallen durchführen.

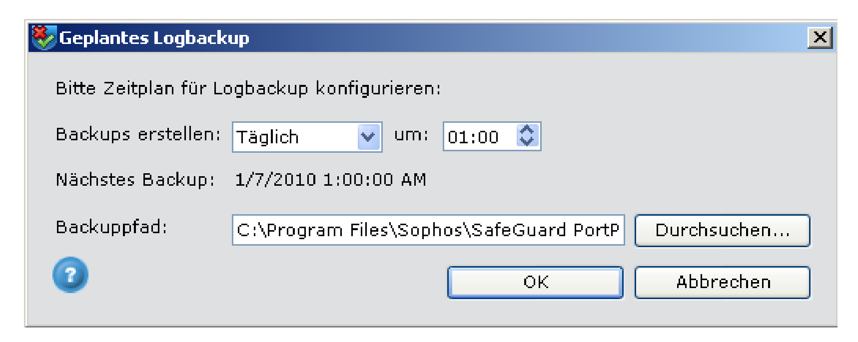
**So führen Sie ein geplantes Backup durch:**

Markieren Sie im Abschnitt *Logbackup* das Kontrollkästchen **Geplante Backups ausführen**. Das Logbackup wird zu den geplanten Zeiten ausgeführt (die nächste geplante Zeit wird angezeigt).

Sie können den Plan für das Logbackup ändern.

**So planen Sie ein Logbackup:**

Klicken Sie im Abschnitt *Logbackup* auf **Ändern**. Das Fenster **Geplantes Logbackup** wird angezeigt:




#### 7.7.1.5.1 Planen von Logbackups

In diesem Fenster können Sie das Intervall (täglich, wöchentlich oder monatlich) und den Zeitpunkt für das geplante Logbackup sowie den Pfad für das Backup festlegen.

**So legen Sie die Backupparameter fest:**

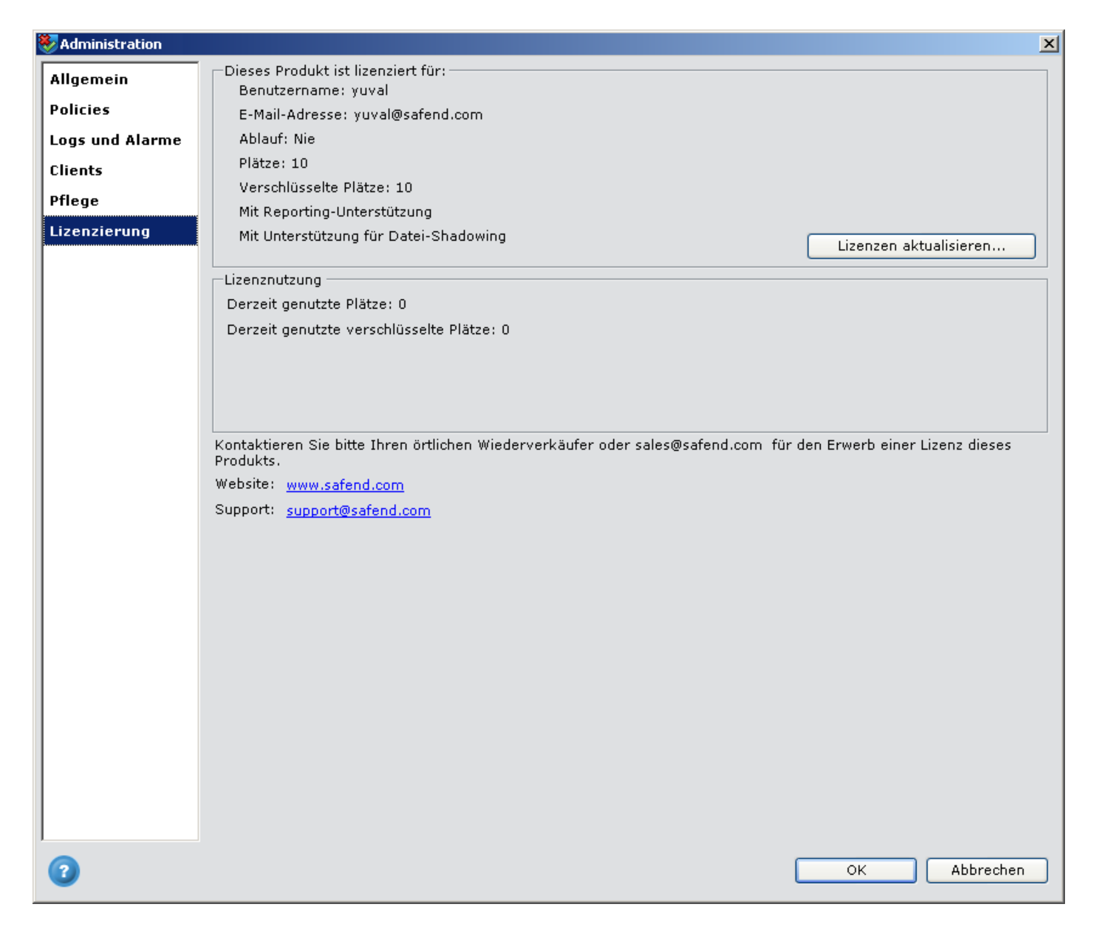
1. Legen Sie das Intervall und die Zeit für die Ausführung unter **Backups erstellen** fest.
2. Klicken Sie auf **Durchsuchen**, um den Pfad für das Backup auszuwählen.
3. Klicken Sie auf **OK**. Der Zeitplan für das Logbackup ist jetzt festgelegt Die Dateien des Logbackups werden gemäß den folgenden Namenskonventionen gespeichert: `LogsBackup01JAN2006_2359.SCB`, wobei 01Jan2006_2359 Datum und Zeit repräsentieren. Die aktuelle Datei wird nicht von der neuen Backupdatei überschrieben, so dass immer zwei Backupdateien vorhanden sind.

## 7.8 Konfigurieren der Inhaltsprüfung

Inhaltsprüfungsdetails werden auf der Registerkarte *Content Inspection* angezeigt und aktualisiert.

## 7.9 Konfigurieren der Einstellungen auf der Registerkarte Lizenzierung

Lizenzdetails werden auf der Registerkarte *Lizenzierung* des Fensters *Administration* angezeigt und aktualisiert:




**Hinweis:** SafeGuard PortProtector bietet verschiedene zusätzliche Funktionen, die durch eine Lizenz aktiviert werden. Diese Zusatzfunktionen sind unter *Dieses Produkt ist lizenziert für:* aufgeführt.

### 7.9.1 Lizenzeinstellungen

Wenn Sie die Anwendung zum ersten Mal öffnen, wird ein Fenster angezeigt, das Sie darüber informiert, dass die Installation in 30 Tagen abläuft. In dieser Zeit sollten Sie Sophos kontaktieren und eine Lizenz für das Produkt erwerben.

Wenn die Lizenz bereits abgelaufen ist, wird eine Meldung angezeigt, und Sie können im System erst dann wieder Operationen ausführen, wenn ein gültiger Lizenzschlüssel eingegeben wurde.

Im Fenster *Administration* werden auf der Registerkarte *Licensing* Lizenzdetails für SafeGuard PortProtector angezeigt. Diese Lizenz kann bei Bedarf aktualisiert werden. Die Registerkarte *Licensing* enthält die folgenden Abschnitte:

- *Lizenzdetails*
- *Lizenznutzung*

**Hinweis:** Bei jeder Änderung einer der Einstellungen auf dieser Registerkarte müssen Sie unten im Fenster *Administration* auf **OK** klicken, damit die Änderungen übernommen werden.

#### 7.9.1.1 Lizenzdetails (Dieses Produkt ist lizenziert für)

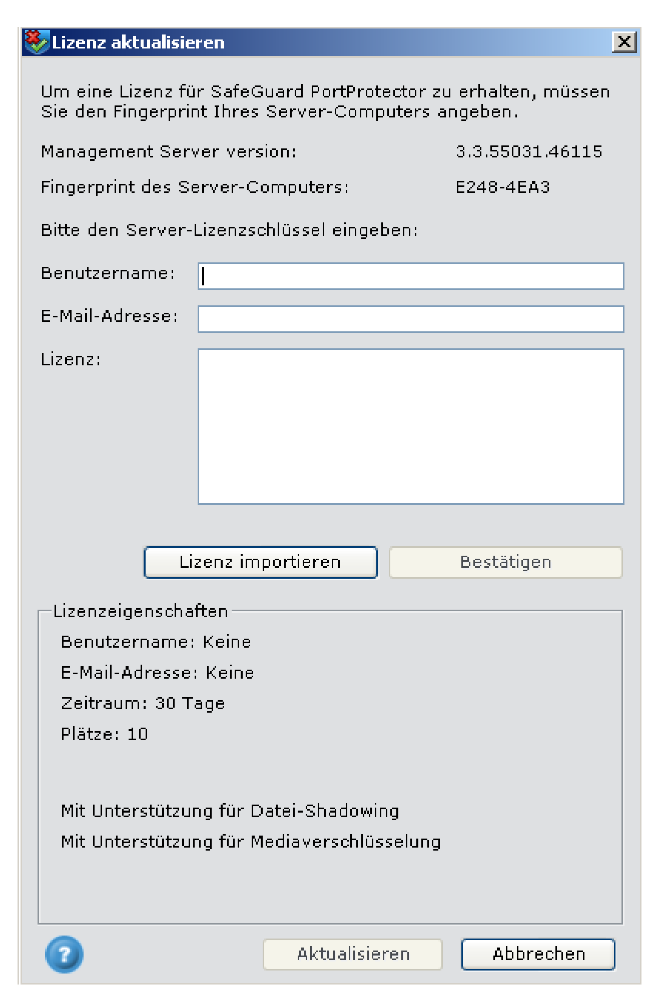
- **Benutzername:** Der Name, der bei der Beschaffung des Produkts benutzt wurde.
- **E-Mail-Adresse:** Die E-Mail-Adresse, die für die Zusendung des Lizenzschlüssels benutzt wurde.
- **Ablauf:** Anzahl der in der Lizenz angegebenen Tage.
- **Plätze:** Anzahl der zulässigen lizenzierten Client-Stationen.
- **Zusatzfunktionen:** Zusatzfunktionen oder Produkte, die zusätzlich zu SafeGuard PortProtector in der Lizenz enthalten sind.

Sie können mittels der Schaltfläche **Lizenz aktualisieren** auf der Registerkarte **Lizenzierung** im Fenster *Administration Settings* einen anderen Lizenzschlüssel eingeben (siehe Abbildung unten).

Bedenken Sie, dass eine neue Lizenz die vorhandene Lizenz überschreibt. Sie wird nicht an Ihre aktuelle Lizenz angehängt. Wenn z. B. Ihre aktuelle Lizenz in einem Jahr abläuft und Sie eine Lizenz für eine weiteres Jahr hinzufügen, haben Sie trotzdem nur eine Ein-Jahres-Lizenz.

**So öffnen Sie das Fenster *Lizenz aktualisieren***

Klicken Sie auf **Lizenz aktualisieren**. Das Fenster wird angezeigt.




**Hinweis:** Wenn die Integration der Inhaltsprüfung aktiviert ist, wird eine zusätzliche Zeile im Abschnitt **Lizenzeigenschaften** angezeigt: "Mit Inhaltsprüfung".

#### 7.9.1.1.1 Aktualisieren der Lizenz

**1 Schritt 1: Lizenzschlüssel beschaffen**

Um einen Lizenzschlüssel zu beschaffen, wenden Sie sich an Sophos oder Ihren Händler, und geben den Fingerprint des Server-Computers so an, wie er auf dem Bildschirm erscheint.

Der Fingerprint in dem oben gezeigten Fenster lautet beispielsweise:

"70AA-6C8F"

Anhand dieses Fingerprints wird ein Lizenzschlüssel für Sie generiert, der nur auf diesem spezifischen Computer benutzt werden kann.

**Hinweis:** Sie können diesen Schlüssel auf keinem anderen Computer verwenden. Wenn Sie Ihren Management Server auf einen anderen Computer migrieren möchten, wenden Sie sich bitte an Ihren Händler oder an den Sophos Support: mailto:support@sophos.com.

2 **Schritt 2: Lizenzschlüssel eingeben**

Gehen Sie folgendermaßen vor:

1 Geben Sie im Feld **Benutzername** Ihren Benutzernamen so ein, wie er in dem Ihnen zugesandten Lizenzschlüssel erscheint.

2 Geben Sie im Feld **E-Mail** Ihre E-Mail-Adresse so ein, wie sie in dem Ihnen zugesandten Lizenzschlüssel erscheint.

3 Geben Sie im Feld **Lizenz** den Lizenzschlüssel ein, den Sie von Sophos erhalten haben.

4 Klicken Sie auf **Bestätigen**. Die **Lizenzeigenschaften** werden angezeigt und geben die aktualisierten Lizenzdaten an, wie etwa die zulässige Anzahl Stationen und den Gültigkeitszeitraum dieser Lizenz. In einigen Fällen wird eine Warnmeldung angezeigt, nachdem Sie auf **Bestätigen** geklickt haben. Diese Meldung weist auf einen ungültigen oder abgelaufenen Lizenzschlüssel hin.

5 Überprüfen Sie die Lizenzdaten, und stellen Sie sicher, dass sie richtig sind.

6 Klicken Sie auf **Aktualisieren**, um die die Lizenz zu aktualisieren.

**Hinweis:** Sobald Sie die Lizenz aktualisiert haben, wird die vorherige Lizenz vollständig entfernt. Seien Sie deshalb bei der Eingabe der Lizenzdaten vorsichtig.

#### 7.9.1.2 Lizenznutzung

Dieses Feld zeigt die Anzahl der Clients, die derzeit vom Management Server bedient werden.

Wenn diese Zahl die Anzahl der lizenzierten Stationen überschreitet, müssen Sie eine neue Lizenz erwerben.

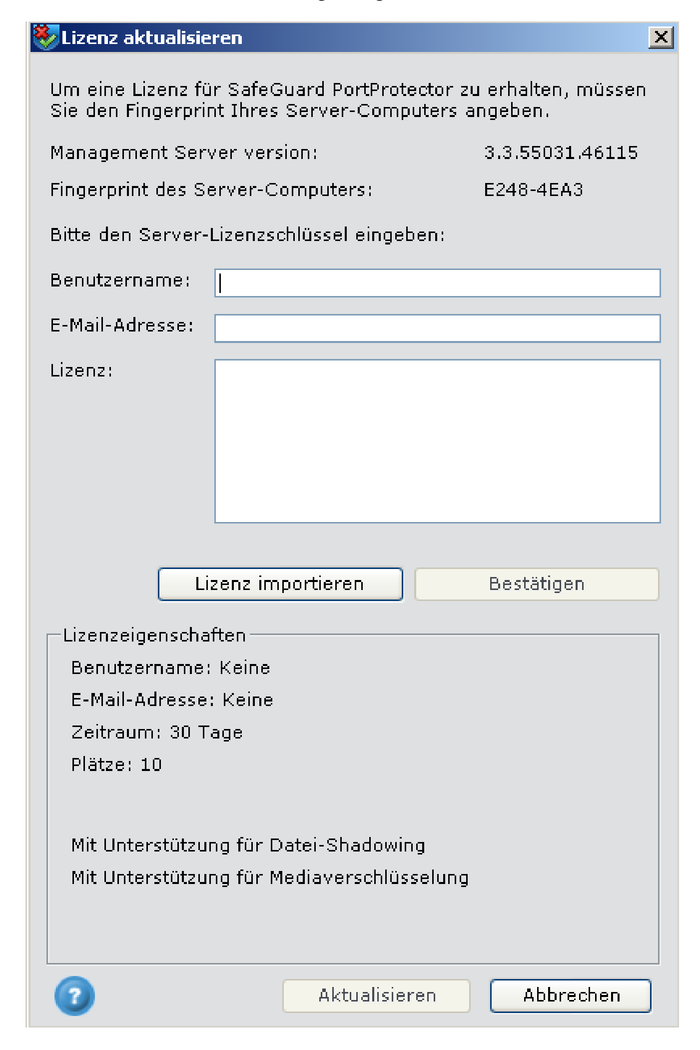
#### 7.9.1.3 Importieren einer externen Evaluierungslizenz

Sie haben die Möglichkeit, eine externe Evaluierungslizenz zu importieren.

**So importieren Sie eine externe Evaluierungslizenz:**

1 Wählen Sie im Menü *Extras* die Option **Administration.**

2 Wählen Sie *Lizenzierung*, und klicken Sie auf **Lizenzen aktualisieren.** Das Dialogfeld *Lizenz aktualisieren* wird angezeigt.




3 Klicken Sie auf **Lizenz importieren.**

4 Wählen Sie die Lizenzdatei (.lic) unter *Lizenz aus einer Datei importieren.*

# 8 Endbenutzer-Erfahrung

## Über dieses Kapitel

SafeGuard PortProtector Client sollte auf den Computer Ihrer Organisation installiert werden, um sie gegen unberechtigte Nutzung ihrer Ports zu schützen. Es ist keine Einrichtung oder Konfiguration des Clients erforderlich, und der Bedienungsaufwand ist bis auf die Verschlüsselung bzw. Entschlüsselung von Wechselspeichergeräten gering.

Weitere Informationen finden Sie in *Durchsetzung der SafeGuard Policy – SafeGuard PortProtector Client* im Kapitel *Einführung in SafeGuard PortProtector*.

Auf einem durch SafeGuard PortProtector geschützten Computer können zwei Anzeigen erscheinen, je nachdem, wie der Administrator die Policy konfiguriert hat, wie in *Schritt 17 Optionen definieren* in *Kapitel 3, Definieren von Policies, beschrieben: Nachrichten und Taskleistensymbole*.

**Hinweis:** Wenn die Client-Sichtbarkeit auf Endpunkten auf den Stealth-Modus (siehe Definieren der Client-Sichtbarkeit auf Endpunkten im Kapitel *Definieren von Policies*) gesetzt ist, bleiben Meldungen und Taskleistensymbol verborgen.

Dieses Kapitel beschreibt die Benutzer-Erfahrung, durch SafeGuard PortProtector Client geschützt zu sein. Es enthält die folgenden Abschnitte:

- ***Meldungen des SafeGuard PortProtector Clients*** beschreibt die Meldungen, die bei der Durchsetzung der SafeGuard PortProtector-Policies erscheinen.
- ***SafeGuard PortProtector Client-Taskleistensymbol*** beschreibt die Zustände des Taskleistensymbols, das das Verhalten des SafeGuard PortProtector Clients repräsentiert.
- ***Optionen des SafeGuard PortProtector Clients*** beschreibt auf dem Client verfügbare Zusatzoptionen, wie etwa die temporäre Aufhebung des Schutzes.
- ***Panik-Modus*** erläutert, woran zu erkennen ist, dass die Policy eines Clients durch Manipulation beschädigt wurde, und was zur Behebung dieses Umstands zu tun ist.
- ***Verschlüsselung und Entschlüsselung von Wechselspeichergeräten*** erläutert, wie Wechselspeichergeräte verschlüsselt werden, wenn die Policy eine Verschlüsselung fordert, und wie verschlüsselte Geräte entschlüsselt werden, um sie auf organisationsfremden Computer zu nutzen, sofern die Policy dies zulässt.
- ***CD/DVD-Verschlüsselung*** erklärt, wie verschlüsselte Volumes erzeugt werden, die Sie auf CD/DVD und externe Festplatten kopieren oder als Container verwenden können, um verschlüsselte Daten auf Ihrer Festplatte zu speichern.

## 8.1 Meldungen des SafeGuard PortProtector Clients

SafeGuard PortProtector-Meldungen erscheinen sofort nach der Installation, je nach den Optionseinstellungen, die für die Policy definiert wurden, die für den Computer/Benutzer gelten. Sobald eine Meldung erscheint, können Sie diese mit einem Klick schließen. Andernfalls verschwindet sie nach einem Moment automatisch. Meldungen zeigen den Portnamen und das Gerätemodell an. Außerdem zeigen Sie den Text an, der in *Schritt 12: Endbenutzer-Meldungen definieren* im Kapitel *Definieren von Policies* erscheint. Hier können Sie den Text auch für die Bedürfnisse Ihrer Organisation modifizieren.

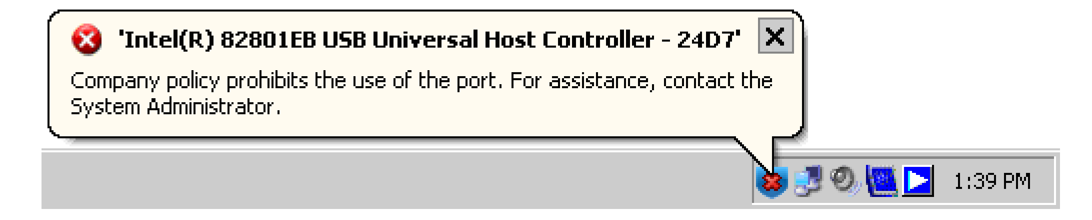
**Hinweis:** Die eindeutige ID spezifischer Geräte wird nicht angezeigt.

Meldungen werden in folgenden Fällen angezeigt (eine Beschreibung der einzelnen Fälle folgt):

- Port gesperrt
- Gerät gesperrt
- Speichergerät gesperrt
- Schreibgeschütztes Speichergerät
- Datei gesperrt
- Dateitransfer-Warnung
- WiFi-Verbindung gesperrt
- Hardware-Keylogger gesperrt
- Policy aktualisiert
- Verschlüsseltes Gerät angeschlossen, Gerät entschlüsseln (Fenster)
- Hibernation sperren

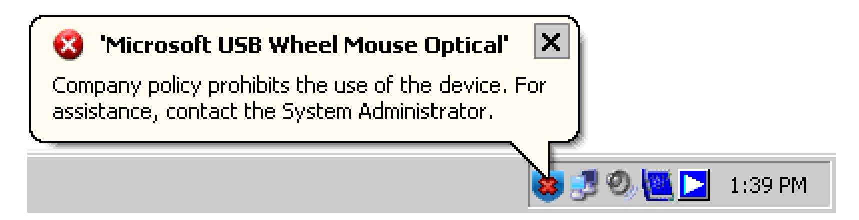
### 8.1.1 Port gesperrt

Eine Meldung wird angezeigt, wenn ein Computer versucht einen als gesperrt definierten Port zu initialisieren. Bei integrierten Ports wird diese Meldung angezeigt, wenn der Endpunkt-Computer neu startet und versucht, den Port zu initialisieren. Sie wird auch angezeigt, wenn ein Adapter für diesen Port an den Endpunkt angeschlossen ist.



## 8.1.2 Gerät gesperrt

Es wird eine Meldung angezeigt, wenn versucht wird, über einen dieser eingeschränkten Ports ein nicht freigegebenes Gerät anzuschließen, was bedeutet, dass weder der Typ, noch das Modell und auch nicht dieses spezifische Gerät freigegeben sind.



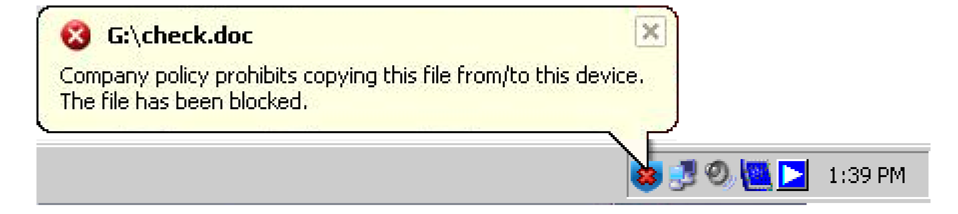

## 8.1.3 Speichergerät gesperrt

Es wird eine Meldung angezeigt, wenn versucht wird, ein Speichergerät anzuschließen, für das weder Typ noch Modell noch das spezifische Gerät freigegeben sind.




## 8.1.4 Datei gesperrt

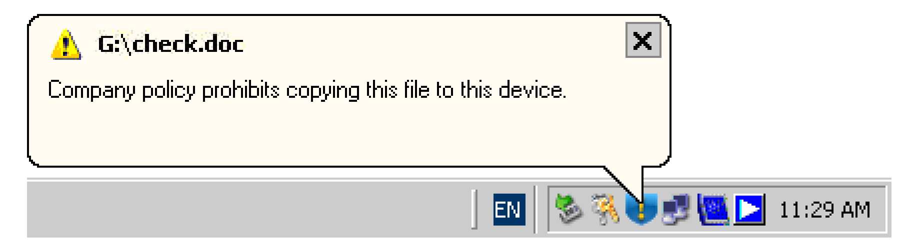
Es wird eine Meldung angezeigt, wenn die Übertragung einer Datei aufgrund der Dateikontrolleinstellungen gesperrt ist.




**Hinweis:** Diese Meldung wird auch angezeigt, wenn eine Datei gesperrt ist, weil die maximale Cache-Größe überschritten wurde.

## 8.1.5 Dateitransfer-Warnung

Es wird eine Meldung angezeigt, wenn eine Datei mit sensiblem Inhalt (eine Datei, die einer Inhaltsprüfung unterzogen wurde) auf ein Speichergerät geschrieben wird.



### 8.1.6 Schreibgeschütztes Speichergerät

Es wird eine Meldung angezeigt, wenn versucht wird, ein Speichergerät anzuschließen, das auf Read-Only-Zugriff gesetzt wurde. Diese Meldung besagt, dass Sie von diesem Speichergerät lesen, aber nicht darauf schreiben können.



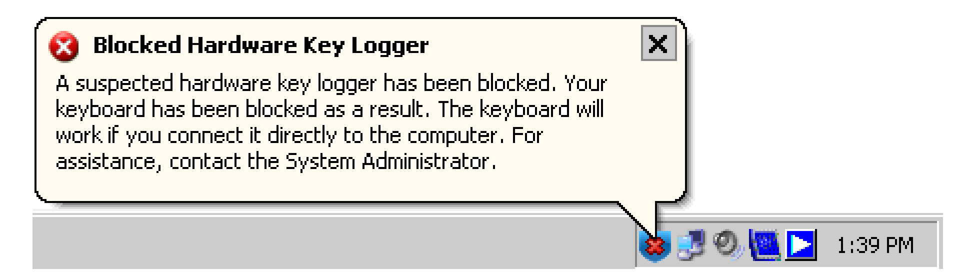

### 8.1.7 WiFi-Verbindung gesperrt

Es wird eine Meldung angezeigt, wenn die WiFi-Verbindung gesperrt ist und versucht wird, den Host mit einem WiFi-Netz zu verbinden. Das würde bedeuten, dass der WiFi-Port eingeschränkt wurde und der Link keinem der Links in der weißen Liste entspricht.



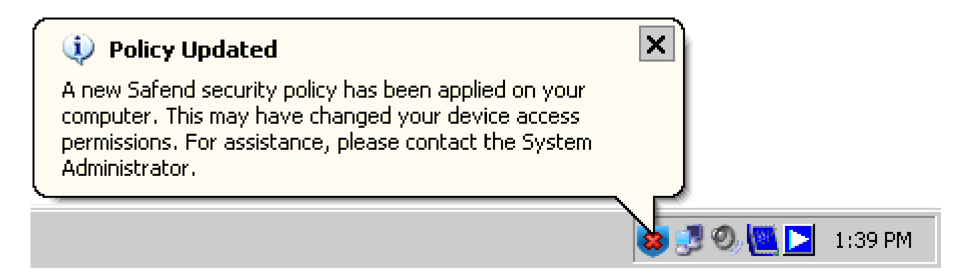

### 8.1.8 Hardware-Keylogger gesperrt

Es wird eine Meldung angezeigt, wenn ein verdächtiger USB Hardware-Keylogger angeschlossen ist. Dadurch wird die Benutzung der Tastatur gesperrt, bis der Key Logger entfernt wird.




### 8.1.9 Policy aktualisiert

Eine Meldung wird angezeigt, wenn dem Computer/Benutzer eine neue Policy zugewiesen wird. Im Folgenden wird beschrieben, wie sich SafeGuard PortProtector verhält, falls die neue Policy einen zuvor zugelassenen Port bzw. ein zuvor zugelassenes Gerät oder Netz sperrt, und umgekehrt.



### 8.1.10 Unverschlüsseltes Gerät angeschlossen, Gerät verschlüsseln

Sobald ein unverschlüsseltes Gerät angeschlossen wird und die Policy eine Verschlüsselung fordert, wird ein Fenster angezeigt. Über dieses Fenster kann das Gerät verschlüsselt werden, wie in *Verschlüsselung und Entschlüsselung von Wechselspeichergeräten* erläutert.




## 8.2 'Zugelassen' zu 'Gesperrt'

Wenn durch eine Policy-Änderung festgelegt wird, dass ein angeschlossenes Gerät jetzt gesperrt ist, ruft SafeGuard PortProtector Client das Betriebssystem auf und fordert, dass das die Verbindung zu dem Gerät unterbrochen wird. Wenn das Gerät derzeit benutzt wird, kann es vorkommen, dass das Betriebssystem nicht dazu in der Lage ist. In *Definieren der Trennung aktiver Geräte* im Kapitel *Definieren von Policies* erfahren Sie, wie sich SafeGuard PortProtector Client in diesem Fall verhält.

## 8.3 'Gesperrt' zu 'Zugelassen'

Wenn durch eine Policy-Änderung festgelegt wird, dass ein gesperrtes Gerät jetzt zugelassen ist, erscheint das Symbol (grünes Kontrollhäkchen). Der SafeGuard PortProtector Client ruft das Betriebssystem und fordert, dass die Verbindung zu dem Gerät hergestellt wird. Auf Endpunkten mit Windows 2000 ist das Betriebssystem gelegentliche nicht dazu in der Lage, und das System muss neu gestartet werden. Dazu werden Sie in einer SafeGuard PortProtector-Meldung aufgefordert, um die Verbindung zu dem Gerät herzustellen.

## 8.4 SafeGuard PortProtector Client-Taskleistensymbol

Auf jedem durch SafeGuard PortProtector geschützten Computer wird ein Taskleistensymbol angezeigt. Es kann ständig oder zeitweilig erscheinen, je nachdem, wie der Administrator die Policy konfiguriert hat, wie in Definieren der Client-Sichtbarkeit auf Endpunkten im Kapitel *Definieren von Policies, beschrieben*.

**Hinweis:** Wenn die Client-Sichtbarkeit auf Endpunkten auf den Stealth-Modus gesetzt ist, bleibt das Taskleistensymbol verborgen.

Wenn Sie den Mauszeiger über das Taskleistensymbol bewegen, werden dieselben Informationen angezeigt, die in der Meldung erscheinen. Bei der Freigabe eines Geräts wird keine Meldung gezeigt, und die Geräteeigenschaften erscheinen hier. Hier einige Beispiele:




- Dies ist das normale SafeGuard PortProtector Client-Taskleistensymbol. Der Administrator kann angeben, dass das SafeGuard PortProtector-Symbol immer in der Taskleiste angezeigt wird, auch wenn SafeGuard PortProtector inaktiv ist. Dadurch wird angezeigt, dass der Computer durch SafeGuard PortProtector geschützt ist.
- Ein Port oder ein angeschlossenes Gerät, der bzw. das zuvor gesperrt war, wurde zugelassen.
- Verschlüsseltes Gerät angeschlossen.
- Nur Lesezugriff.
- Es wurde versucht, einen Port oder ein Gerät zu benutzen, der/das gesperrt ist.
- Client-Schutz aufgehoben.
- Endbenutzereingabe für Wechselspeichergerät erforderlich.
- Offline Access Utility.

Mit Ausnahme des ersten Symbols (normales SafeGuard PortProtector Client-Symbol) werden die Symbole einen Moment lang angezeigt und kehren dann zurück zum ersten Symbol.

### 8.4.1 Modi der Client-Sichtbarkeit

Standardmäßig wird das SafeGuard PortProtector Symbol immer in der Taskleiste eines geschützten Computers angezeigt. Dadurch kann der Administratoren auf einen Blick erkennen, dass ein Computer durch SafeGuard PortProtector geschützt ist.

Einige Administratoren ziehen es jedoch vor, die Sichtbarkeit von SafeGuard PortProtector Client auf den Endpunkten auf ein Minimum zu reduzieren. Es stehen drei verschiedene Sichtbarkeitsmodi zur Verfügung:

- **Voll sichtbar –** Das SafeGuard PortProtector-Taskleistensymbol und Ereignismeldungen immer anzeigen. Dies ist der Standardmodus.
- **Teilweise sichtbar –** Das SafeGuard PortProtector-Taskleistensymbol bei Inaktivität ausblenden, aber Ereignismeldungen anzeigen. In diesem Modus wird das Symbol kurz angezeigt, wenn ein Gerät angeschlossen wird, und verschwindet danach wieder.
- **Stealth-Modus –** Das Taskleistensymbol von SafeGuard PortProtector ausblenden und keine Ereignismeldungen anzeigen. In diesem Modus wird der Endbenutzer das Symbol nie sehen und auch nie Meldungen zu gesperrten Geräten/Ports erhalten.

**Hinweis:** Wenn Sie in Ihre Organisation eine Verschlüsselung nutzen, sollte der Stealth-Modus nicht genutzt werden, um die erforderlichen Meldungen anzuzeigen, sobald ein unverschlüsseltes Gerät angeschlossen wird.

Diese Optionen werden in Definieren der Client-Sichtbarkeit im Kapitel *Definieren von Policies*, konfiguriert.

## 8.5 Optionen des SafeGuard PortProtector Clients

Neben dem ständigen Schutz und laufender Überwachung der Host-Computer kann der Endbenutzer mit SafeGuard PortProtector Client weitere Aktionen auf dem Host-Computer ausführen:

- ***Aktualisieren der Client-Policy*** weist den Client an, die ihn schützende Policy nach einer Policy-Änderung zu aktualisieren.
- ***Aufheben des SafeGuard PortProtector-Schutzes auf einem*** Client hebt den SafeGuard PortProtector Schutz auf dem Host-Computer zeitweilig auf.
- ***Anzeigen und Ausblenden von Dateimeldungen*** ermöglicht Endbenutzern das Ausblenden und erneute Anzeigen von Dateimeldungen, wenn sie seine Arbeit behindern.
- ***Erstellen eines virtuellen verschlüsselten Volumes*** ermöglicht Endbenutzern das Erstellen verschlüsselter Container, die auf CD/DVD und externe Festplatten kopiert werden können.
- ***Administrative Aufgaben*** ermöglicht dem Administrator das Ausführen von Tasks wie etwa Aufhebung des Schutzes oder Zurücksetzen der Tastatur, wenn ein Key Logger vermutet und gesperrt wurde.

Diese Aktionen werden im *SafeGuard PortProtector* Client-Fenster ausgeführt.

**So öffnen Sie das *SafeGuard PortProtector Client*-Fenster:**

1 Doppelklicken Sie auf das SafeGuard PortProtector-Taskleistensymbol.

ODER

Klicken Sie mit der rechten Maustaste auf das SafeGuard PortProtector-Taskleistensymbol und wählen Sie **Optionen**.

ODER

Doppelklicken Sie in der Windows *Systemsteuerung* auf das SafeGuard PortProtector-Symbol (wenn das SafeGuard PortProtector-Taskleistensymbol nicht sichtbar ist, kann nur diese Option genutzt werden).

2 Das SafeGuard PortProtector Client-Fenster wird angezeigt:




Dieses Fenster enthält drei Registerkarten:

- *General*: Liefert allgemeine Informationen (Hostname, Softwareversion und Servername). Darüber hinaus werden Informationen zur Policy angezeigt (aktueller Policy-Name, Angaben darüber, ob die Policy auf den Computer oder aktuellen Benutzer angewandt wird, sowie Datum und Uhrzeit der letzten Policy-Aktualisierung). Des Weiteren werden Informationen zum Schutzstatus angezeigt, die darüber informieren, ob der Computer derzeit geschützt ist oder ob der Schutz aufgehoben ist. Außerdem werden Informationen zum Inhaltsprüfungsstatus geliefert, der Aufschluss darüber gibt, ob die Inhaltsprüfung ein- oder ausgeschaltet ist.
- *Extras*: Liefert Informationen zur Geräteverschlüsselung und ermöglicht es, Dateimeldungen auf dem Desktop auszublenden. Weitere Informationen finden Sie im Abschnitt *Erstellen und Benutzen eines verschlüsselten Volumes*.
- *Info*: Liefert allgemeine Informationen zu SafeGuard PortProtector Client.

Das Fenster enthält auch mehrere Schaltflächen, die nachstehend besprochen werden.

### 8.5.1 Aktualisieren der Client-Policy

Die Policy eines SafeGuard PortProtector Clients wird in einem Vorgang aktualisiert, bei dem der Client den Management Server, GPO-Dienst oder die Registry-Datei (je nach dem von Ihnen gewählten Verfahren für die Policy-Verteilung) in vordefinierten Intervallen prüft und die Policy aktualisiert, falls sie sich geändert hat. *Aktualisieren einer Policy auf einem Client* im Kapitel *Verwalten von Clients* erläutert, wie SafeGuard PortProtector Clients benachrichtigt werden, ihre Policy zum frühestmöglichen Zeitpunkt über die SafeGuard PortProtector Management Console zu aktualisieren. Bei einem einzelnen, spezifischen Client ist dies auch vom Host-Computer aus möglich.

**So aktualisieren Sie eine Policy vom Host-Computer aus:**

Klicken Sie auf der Registerkarte *Allgemein* im *SafeGuard PortProtector Client*-Fenster auf **Jetzt aktualisieren**. Wenn eine aktualisierte Policy gefunden wird, wird eine Meldung 'Policy Updated' angezeigt.

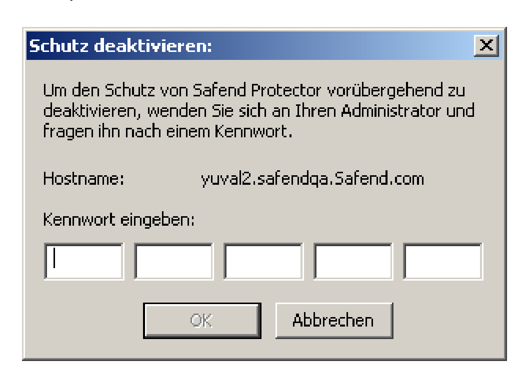
### 8.5.2 Aufheben des SafeGuard PortProtector-Schutzes auf einem Client

Wie im Kapitel *Verwalten von Clients*, erläutert, können Sie den SafeGuard PortProtector Schutz temporär auf einem Client aufheben, ohne die Anwendung deinstallieren zu müssen. Dazu erzeugen Sie in der Management Console ein Suspendierungskennwort, das Sie dem Benutzer zur Verfügung stellen und das er dann zur Aufhebung des Schutzes eingibt. Mit dieser Option können Sie den Schutz für bis zu einer Woche aufheben. Im nächsten Abschnitt wird erläutert, was auf Client-Seite getan werden muss. Darüber hinaus kann der Systemadministrator selbst den Schutz ad-hoc kurzzeitig (nicht länger als einen Tag) aufheben. Beide Optionen werden im Folgenden erläutert.

#### 8.5.2.1 Aufhebung des Schutzes durch den Benutzer

**So heben Sie als Benutzer den SafeGuard PortProtector Schutz auf:**

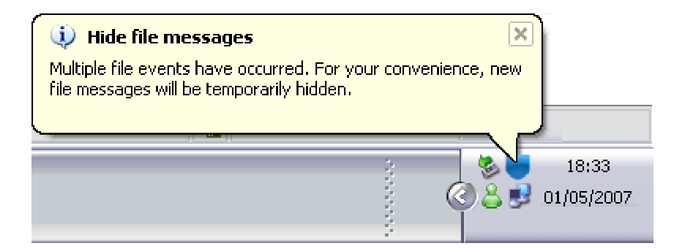
1 Klicken Sie auf der Registerkarte *Allgemein* im *SafeGuard PortProtector Client*-Fenster auf **Jetzt deaktivieren**. Das Fenster *Schutz deaktivieren* wird angezeigt.



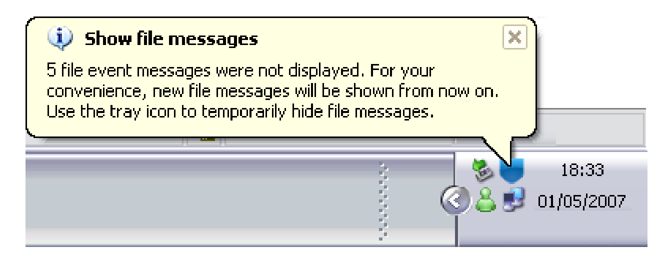

2 Geben Sie das Suspendierungskennwort ein, das Sie vom Administrator erhalten haben, und klicken Sie auf **OK.** Es wird eine Meldung angezeigt, die den Zeitraum der Aufhebung angibt. Der SafeGuard PortProtector Schutz wird auf dem Host für die vom Systemadministrator bei der Generierung des Suspendierungskennworts definierten Zeitraum aufgehoben. Nach Ablauf dieses Zeitraums wird der Schutz automatisch wieder hergestellt.

## 8.5.3 Anzeigen und Ausblenden von Dateimeldungen

Wie weiter oben in diesem Kapitel erläutert, werden Dateimeldungen immer dann angezeigt, wenn ein Dateitransfer gesperrt ist oder eine Datei mit sensiblem Inhalt auf ein Speichergerät übertragen wird. In manchen Fällen können diese Meldungen zu häufig auftreten und so den Endbenutzer bei seiner laufenden Arbeit stören. Wenn SafeGuard PortProtector Client dies feststellt (gemäß hartcodierter Definitionen), wird die Anzeige der Dateimeldungen gestoppt und die folgende Meldung angezeigt:




Wenn SafeGuard PortProtector Client feststellt, dass die Häufigkeit der Dateimeldungen keine Störung mehr darstellt (gemäß hartcodierter Definitionen), wird die folgende Meldung angezeigt:




Darüber hinaus kann der Endbenutzer die Dateimeldungen jederzeit ausblenden oder anzeigen, wenn der hartcodierte Schwellenwert ungeeignet ist.

**So blenden Sie Dateimeldungen manuell aus:**

Klicken Sie auf der Registerkarte *Extras* im *SafeGuard PortProtector Client*-Fenster auf **Hide File Messages**

ODER

Klicken Sie mit der rechten Maustaste auf das SafeGuard PortProtector Client-Taskleistensymbol und wählen Sie **Hide File Messages**

Ab diesem Zeitpunkt werden keine Dateimeldungen mehr gezeigt, bis der Endbenutzer wählt, sie wieder anzuzeigen.

**So zeigen Sie Dateimeldungen manuell an:**

Klicken Sie auf der Registerkarte *Tools* im *SafeGuard PortProtector Client*-Fenster auf **Show File Messages**

ODER

Klicken Sie mit der rechten Maustaste auf das SafeGuard PortProtector Client-Taskleistensymbol und wählen Sie **Show File Messages**

Ab diesem Zeitpunkt werden Dateimeldungen angezeigt.

### 8.5.4 Erstellen eines virtuellen verschlüsselten Volumes

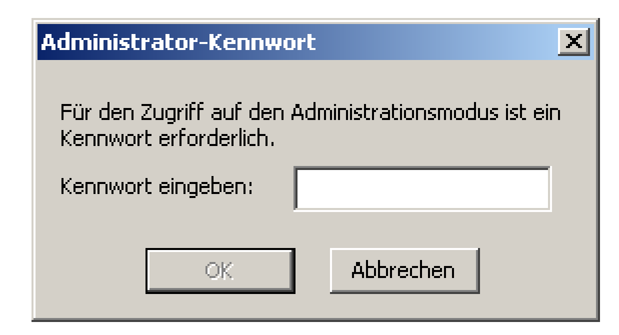
Über diese Option können Endbenutzer verschlüsselte Container erstellen, die auf CD/DVD und externe Festplatten kopiert werden können. Detaillierte Informationen hierzu finden Sie in *CD/DVD-Verschlüsselung*.

### 8.5.5 Administrative Aufgaben

Auf den Endpunkten stehen einige administrative Optionen zur Verfügung. Über diese Optionen kann der Administrator eingeschränkt und unter Verwendung des Client Administration Password, das Sie in der Policies-Welt definiert haben, Funktionen ausführen.

So wechseln Sie in den Administration-Modus:

1 Klicken Sie unten auf der Registerkarte *General* im *SafeGuard PortProtector Client*-Fenster auf **Administrationsmodus.** Das Fenster *Administrator-Kennwort* wird angezeigt.




2 Geben Sie das Client Administration Kennwort ein, und klicken Sie auf **OK.**

3 Das Fenster bietet jetzt zwei Administrationsfunktionen an:

- Administrator-Deaktivierung
- Tastaturen zurücksetzen




4 Nachdem Sie die gewünschten Funktionen ausgeführt haben, klicken Sie auf **Schließen**, um das *SafeGuard PortProtector Client*-Fenster zu schließen.

5 Sobald Sie dieses Fenster das nächste Mal öffnen, zeigt es erst dann Administrationsfunktionen an, wenn der Administrator das Client Administration Password eingegeben hat.

**Hinweis:** Denken Sie immer daran, das *SafeGuard PortProtector Client*-Fenster nach der Ausführung der administrativen Aufgaben zu schließen. Andernfalls können unbefugte Benutzer Administrationsfunktionen ausführen. Nachdem Sie das Fenster geschlossen haben, müssen Sie Ihr Administrationskennwort wieder eingeben, um Administrationsfunktionen ausführen zu können.

#### 8.5.5.1 Aufhebung des Schutzes durch den Systemadministrator

Wenn Sie (der Administrator) den SafeGuard PortProtector Schutz auf einem Client ad-hoc aufheben müssen, können Sie hierfür das Client-Administrationskennwort nutzen.

So heben Sie den Schutz auf dem Client auf:

1 Wechseln Sie in den Administration-Modus (wie beschrieben).

2 Klicken Sie im Abschnitt **Schutzstatus** im *SafeGuard PortProtector Client*-Fenster (unterer Abschnitt) auf **Administrator-Deaktivierung**. Der Schutz wird aufgehoben.

3 Klicken Sie auf **Resume Now** im Abschnitt **Schutzstatus**, um den Schutz wieder herzustellen.

4 Schließen Sie das *SafeGuard PortProtector Client*-Fenster.

**Hinweis:** Falls Sie vergessen, den Schutz wieder herzustellen, wird er automatisch 24 Stunden nach der Aufhebung wieder hergestellt.

**Hinweis:** Denken Sie immer daran, das *SafeGuard PortProtector Client*-Fenster nach der Ausführung der administrativen Aufgaben zu schließen. Andernfalls können unbefugte Benutzer Administrationsfunktionen ausführen. Nachdem Sie das Fenster geschlossen haben, müssen Sie Ihr Administrationskennwort wieder eingeben, um Administrationsfunktionen ausführen zu können.

#### 8.5.5.2 Zurücksetzen von Tastaturen (Tastatur-Hubs freigeben)

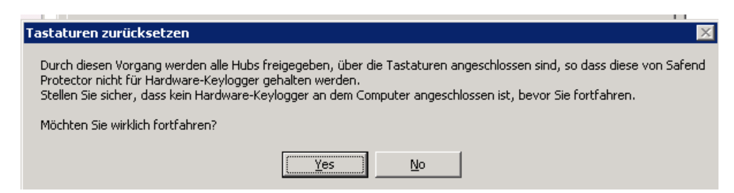
*Schritt 5: Gerätekontrolle definieren* im Kapitel *Definieren von Policies*, beschreibt, wie eine Policy Computer gegen Hardware-Keylogger schützen kann. Damit können Sie eine Tastatur sperren, wenn SafeGuard PortProtector den Verdacht hat, dass ein Hardware-Keylogger angeschlossen ist. In einigen Fällen, wenn eine Tastatur über ein Hub (eins oder mehrere) angeschlossen ist, kann SafeGuard PortProtector Management das Hub fälschlicherweise für einen Keylogger halten und die Tastatur sperren. Durch das "Zurücksetzen der Tastatur" werden die die Hubs freigegeben, über die die Tastatur zum Zeitpunkt des Zurücksetzens angeschlossen ist (siehe nachfolgende Beschreibung).

**Hinweis:** Vor dem Zurücksetzen der Tastatur müssen Sie sich vergewissern, dass kein Keylogger mehr angeschlossen ist, da dieser ansonsten freigegeben würde.

**So setzen Sie Tastaturen zurück:**

1 Wechseln Sie in den Administration-Modus (wie beschrieben)

2 Klicken Sie im Abschnitt Protection Status im *SafeGuard PortProtector Client*-Fenster (unterer Abschnitt) auf **Tastaturen zurücksetzen.** Das Fenster *Tastaturen zurücksetzen* wird angezeigt



3 Vergewissern Sie sich, dass kein Hardware-Keylogger zwischen der Tastatur und dem Computer angeschlossen ist.

4 Klicken Sie im Fenster *Tastaturen zurücksetzen* auf **OK**. Alle Hubs, über die die Tastatur angeschlossen ist, werden jetzt freigegeben, und die Tastatur funktioniert wieder.

**Hinweis:** Denken Sie immer daran, das *SafeGuard PortProtector Client*-Fenster nach der Ausführung der administrativen Aufgaben zu schließen. Andernfalls können unbefugte Benutzer Administrationsfunktionen ausführen. Nachdem Sie das Fenster geschlossen haben, müssen Sie Ihr Administrationskennwort wieder eingeben, um Administrationsfunktionen ausführen zu können.

## 8.6 Panik-Modus

Wenn ein Client manipuliert wird, wechselt er in den Panik-Modus und sperrt alle Ports. Wenn das passiert, wird im *SafeGuard PortProtector Client*-Fenster die folgende Meldung im Abschnitt *Schutzstatus* angezeigt: "Panic (machine policy corrupted) ". Es kann ein Logereignis 'Ungültige Policy' ausgegeben werden, wenn einige Teile der Policy noch intakt sind. Wenn sie aber total beschädigt ist, kann kein Log mehr gesendet werden.

Um den Panik-Modus zu beenden, wenden Sie einfach eine gültige Policy auf den Client an.

## 8.7 Verschlüsselung und Entschlüsselung von Wechselspeichergeräten

SafeGuard PortProtector ermöglicht es den Endbenutzern, Wechselspeichergeräte und externe Festplatten zu verschlüsseln. Auf diese Weise wird nicht nur sichergestellt, dass Verlust oder Diebstahl des verschlüsselten Geräts keinen Schaden für die Organisation bedeuten, sondern auch ein Durchsickern von Informationen verhindert. In der Regel kann ein verschlüsseltes Speichergerät nur in der Organisationsumgebung genutzt werden. Zudem ist eine explizite Autorisierung erforderlich, um es auf organisationsfremden Computern zu nutzen.

In einigen Fällen kann die Endpunkt-Policy vorschreiben, dass ein solches Speichergerät verschlüsselt sein muss. Alternativ kann der Endbenutzer beschließen, ein Speichergerät zu verschlüsseln, auch wenn die Policy dies nicht fordert.

Falls die Policy eine Verschlüsselung fordert und ein Benutzer ein unverschlüsseltes Gerät anschließt, wird das Gerät entweder gesperrt oder erhält nur Lesezugriff, abhängig von den Policy-Einstellungen (siehe *Schritt 13: Mediaverschlüsselung definieren* im Kapitel *Definieren von Policies)*. Gleichzeitig erhält der Benutzer ist Gegeben die Möglichkeit, das Gerät zu verschlüsseln, um es benutzen zu können. Dies ist in *Verschlüsseln eines Geräts erläutert.*

Eine Policy kann auch autorisierten Benutzern mittels Entschlüsselung Zugriff auf ein organisatorisch verschlüsseltes Gerät auf einem organisationsfremden Computer gewähren. Dies ist in *Offline-Zugriff auf verschlüsselte Geräte erläutert.*

**Hinweis:** Organisatorisch verschlüsselte Wechselspeichergeräte und externe Festplatten können auf jedem durch SafeGuard PortProtector geschützten Computer der Organisation genutzt werden, auch auf denen, deren geltende Policy keine Verschlüsselung erfordert.

### 8.7.1 Verschlüsseln eines Geräts

Wie zuvor erwähnt können Wechselspeichergeräte und externe Festplatten verschlüsselt werden, unabhängig davon, ob die Endpunkt-Policy dies verlangt oder nicht.

Falls die Policy eine Verschlüsselung fordert und ein unverschlüsseltes Gerät an den Computer angeschlossen wird, wird das Gerät entweder gesperrt oder erhält nur Lesezugriff, je nach Policy-Einstellungen (siehe *Mediaverschlüsselung definieren* im Kapitel *Definieren von Policies)*. Um das Gerät voll nutzen zu können, muss es von einem durch SafeGuard PortProtector geschützten Computer in Ihrer Organisation verschlüsselt werden. Wenn ein unverschlüsseltes Gerät angeschlossen wird, erscheint ein Fenster, das den Benutzer darüber informiert und ihn auffordert, das Gerät zu verschlüsseln.




Falls die Policy keine Verschlüsselung erforderlich macht, kann das Gerät dennoch verschlüsselt werden. In diesem Fall erscheint jedoch keine Endbenutzer-Meldung.

**So verschlüsseln Sie ein Wechselspeichergerät oder eine externe Festplatte, falls die Policy dies verlangt:**

**Hinweis:** Die Schritte zum Verschlüsseln eines Wechselspeichergeräts sind dieselben, ganz gleich ob Sie *Geräte-Volumeverschlüsselung* oder *Geräte-Speicherverschlüsselung* gewählt haben.

1 Klicken Sie im Fenster *Ein Gerät versucht, eine Verbindung zu Ihrem Computer herzustellen*, das angezeigt wird, wenn Sie das Gerät anschließen, auf **Verschlüsseln.** Das folgende Fenster wird für ein Wechselspeichergerät angezeigt:



**Hinweis:** Falls Sie nicht genügend Zeit hatten, auf das Fenster *Unverschlüsseltes Gerät angeschlossen* zu klicken, und es ausgeblendet wurde, folgen Sie den nachfolgenden Anleitungen für das Verschlüsseln eines Geräts, wenn kein Fenster angezeigt wird.

2 Aktivieren Sie die entsprechende Optionsschaltfläche, ob Sie die die Daten auf dem Gerät sichern und wiederherstellen möchten, oder ob sie vorhandenen Daten auf dem Gerät löschen möchten (diese Angabe ist erforderlich, weil das Gerät beim Verschlüsseln formatiert wird).

3 Klicken Sie auf **Weiter**.

4 Das folgende Fenster wird für eine externe Festplatte angezeigt:




**Hinweis:** Es wird dringend empfohlen, die Daten auf dem Gerät zu sichern, bevor Sie mit der Verschlüsselung fortfahren.

5 Klicken Sie auf **Weiter**.

6 Wenn Sie über die Rechte verfügen, ein Kennwort für den Offline-Zugriff auf Speichergeräte festzulegen, wird das folgende Fenster angezeigt.




7 Geben Sie das Kennwort ein, das auf Computern außerhalb Ihrer Organisation eingegeben werden muss, um auf den Inhalt zuzugreifen. Falls Sie das Kennwort vergessen haben, können Sie jederzeit ein neues Kennwort festlegen.

**Hinweis:** Es ist zwingend erforderlich, ein Kennwort festzulegen, um den Offline-Zugriff zu ermöglichen, damit das Gerät außerhalb der Organisation genutzt werden kann. Das von Ihnen festgelegte Kennwort muss den Kennwortregeln in Ihrer Organisation entsprechen. Das Kennwort für den Offline-Zugriff kann auch wie in *Festlegen eines Kennworts für den Offline-Zugriff* beschrieben festgelegt werden.

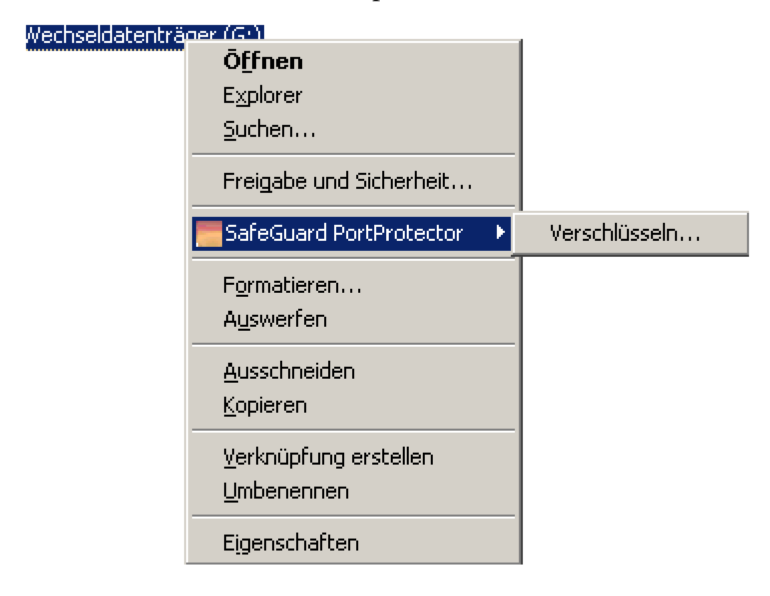
8 Der Verschlüsselungsvorgang (einschließlich Backup und Wiederherstellung, falls ausgewählt) beginnt, und es wird eine Verlaufsanzeige angezeigt. Sobald der Verschlüsselungsvorgang beendet ist, wird folgende Meldung angezeigt:



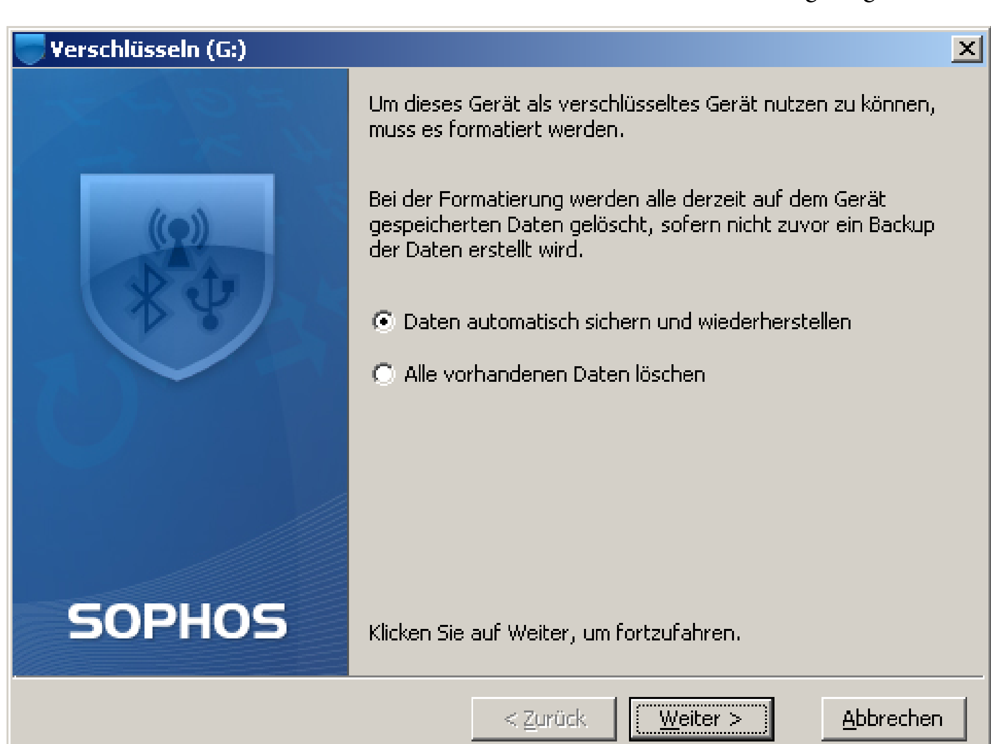

9 Klicken Sie auf **Fertig stellen.** Das Gerät ist jetzt verschlüsselt und die darauf gespeicherten Daten sind im Falle eines Verlustes oder Diebstahls geschützt.
Verschlüsselte Geräte werden durch ein spezielles Symbol gekennzeichnet (ein blaues Schloss), wie in Removable Disk (E:).

**So verschlüsseln Sie ein Wechselspeichergerät, wenn kein Endbenutzer-Fenster angezeigt wird:**

1 Wenn die Meldung verschwunden ist (sie wird nur ein paar Sekunden lang angezeigt), oder die Policy keine Verschlüsselung fordert (so dass keine Meldung angezeigt wird), öffnen Sie in Windows Explorer **Mein Computer** und klicken Sie mit der rechten Maustaste auf das Gerät. Die Option **SafeGuard PortProtector** wird im Kontextmenü angezeigt, und das Untermenü enthält die Option **Verschlüsseln**, wie in der folgenden Abbildung gezeigt:



2 Klicken Sie auf **Verschlüsseln**. Das Fenster *Verschlüsseln* wird angezeigt:




3 Fahren Sie ab Schritt 2 oben in *Verschlüsseln eines Geräts* fort.

## 8.7.2 Online-Zugriff auf verschlüsselte Geräte

Der Administrator kann eine Policy festlegen, mit der die Benutzer zur Eingabe eines Kennworts innerhalb der Organisation gezwungen werden, um auf Geräte zuzugreifen, die von irgendjemandem in der Organisation verschlüsselt wurden (selbst Geräte, die sich selbst verschlüsselt haben).

Von diesem Zeitpunkt an werden sie aufgefordert, das Gerätekennwort jedes Mal einzugeben, wenn der Benutzer das verschlüsselte Gerät an einen geschützten Computer in derselben Organisation anschließt (vorausgesetzt, die entsprechende Policy gilt).



Auf das Gerät kann nur nach Eingabe des richtigen Kennworts zugegriffen werden.

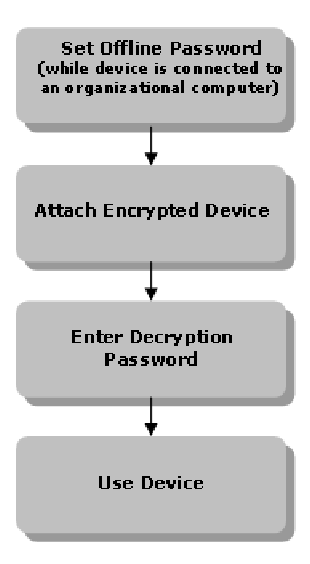
Weitere Informationen hierzu finden Sie in Definieren der Mediaverschlüsselungseinstellungen.

Falls ein Benutzer ein Kennwort vergisst, kann der Administrator das Gerätekennwort ändern. Dazu ist die temporäre Aufhebung des Client-Schutzes erforderlich. Während der Client-Suspendierung kann der Benutzer auf Geräte zugreifen und ein Gerätekennwort ändern, ohne ein Kennwort einzugeben. Auf diese Weise kann also ein Benutzer mit Unterstützung durch den Administrator ein neues Kennwort für das Gerät festlegen.

Weitere Informationen hierzu finden Sie in Aufheben des SafeGuard PortProtector-Schutzes auf einem Client.

## 8.7.3 Offline-Zugriff auf verschlüsselte Geräte

In der Regel können organisatorisch verschlüsselte Wechselspeichergeräte nur benutzt werden, wenn sie an Computer angeschlossen werden, die durch Organisation SafeGuard PortProtector Clients geschützt sind. Dennoch können Benutzer, sofern die geltende Policy des Endbenutzers es zulässt (siehe Schritt *13: Mediaverschlüsselung definieren* im Kapitel *Definieren von Policies*), auch auf ein Wechselspeichergerät auf firmenfremden Computern zugreifen. Um auf verschlüsselte Geräte auf organisationsfremden Computern zuzugreifen, müssen folgende Schritte ausgeführt werden:




Der Vorgang wird im Folgenden beschrieben.

### 8.7.3.1 Festlegen eines Kennworts für den Offline-Zugriff

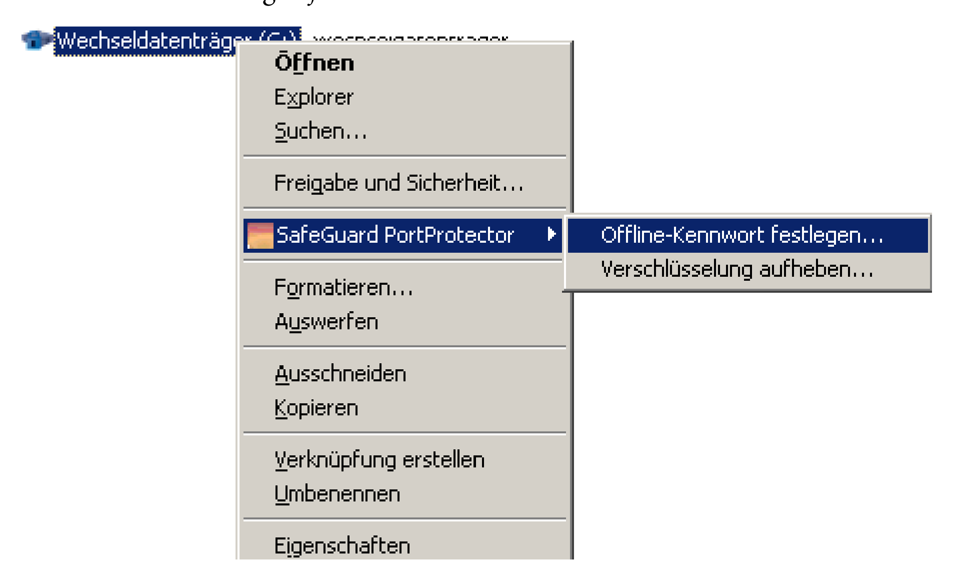
**Hinweis:** Wenn Sie während des Verschlüsselungsvorgangs *Zugriffskennwort festlegen* wählen, ist dieser Schritt nicht erforderlich.

Wenn die geltende Policy des Endbenutzers es die Nutzung von verschlüsselten Geräten auf firmenfremden Computern zulässt, kann ein Kennwort für den Offline-Zugriff (Entschlüsselung) festgelegt werden, das für den Offline-Zugriff auf das Gerät genutzt wird.

**So legen Sie ein Kennwort für den Offline-Zugriff (Entschlüsselung) fest:**

1 Schließen Sie das Gerät, auf das Sie offline zugreifen möchten, an Ihren durch SafeGuard PortProtector geschützten Computer an.

2 Klicken Sie in Mein Computer mit der rechten Maustaste auf das Gerät, und wählen Sie die Shell-Erweiterung *SafeGuard PortProtector*:




3 Klicken Sie auf **Offline-Kennwort festlegen.** Das Fenster *Offline-Kennwort festlegen* wird angezeigt:



4 Legen Sie in diesem Fenster ein Kennwort fest, bestätigen Sie es, und klicken Sie auf **Weiter**. Das folgende Fenster wird angezeigt:




5 Klicken Sie auf **Beenden**. Jetzt ist ein Offline-Zugangskennwort für das angeschlossene Wechselspeichergerät festgelegt.

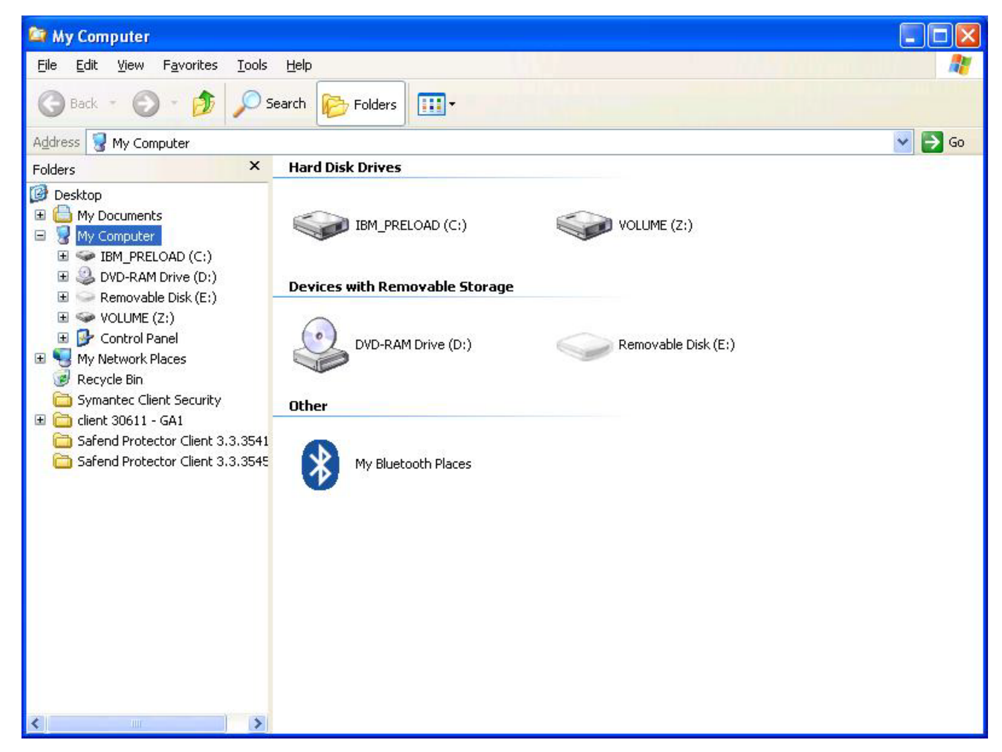
**Hinweis:** Das von Ihnen festgelegte Kennwort muss den Kennwortregeln in Ihrer Organisation entsprechen. Wenn Sie das Kennwort für den Offline-Zugriff vergessen haben oder ändern möchten, können Sie jederzeit ein neues Kennwort festlegen.

#### 8.7.3.2 Online Zugriff auf volumeverschlüsselte Geräte

Hinweis: Eine Beschreibung des Offline-Zugriffs bei ausgewählter Partitionsverschlüsselung finden Sie im Abschnitt *Offline-Zugriff auf partitionsverschlüsselte Geräte*.

Die Option der Verschlüsselung des Geräte-Volumes ermöglicht den Offline-Zugriff auf Speichergeräte durch befugte Benutzer. Lokale Administrationsrechte sind hierfür nicht erforderlich. Die Dateien, auf die auf diese Weise zugegriffen wird, können nur über die Option 'Speichern unter' geändert werden. Zudem kann nicht mit einer anderen Anwendung oder von einer Befehlszeile auf die Dateien zugegriffen werden, bevor sie auf dem lokalen (ungeschützten) Computer mit 'Speichern unter' unter einem anderen Namen gespeichert wurden. Dieses Verhalten ähnelt dem eines E-Mail-Anhangs oder einem komprimierten Windows-Ordner.

Nach der Verschlüsselung erscheint das volumeverschlüsselte Gerät, das an einen Computer angeschlossen ist, auf dem Safend Protector läuft, in Mein Computer:




Sie sehen 2 Symbole:

- **Für ein DOK:** Plattenvolume (z) erscheint unter Festplattenlaufwerke und ein abgedunkeltes Symbol erscheint unter Geräte mit Wechselspeicher.
- Für ein externes Festplattenlaufwerk: Beide Symbole erscheinen unter Festplattenlaufwerke.

**So greifen Sie offline auf ein volumeverschlüsseltes Gerät zu (auf ungeschütztem Computer):**

1 Schließen Sie das verschlüsselte Gerät (für das ein Kennwort für den Offline-Zugriff festgelegt wurde) an den ungeschützten Computer an. Auf diesem Laufwerk werden zwei Dateien angezeigt: AcessSecureData.exe und MyVolume.ses



| Name | Size | Type | Date Modified |
|---|---|---|---|
| AccessSecureData | 6,220 KB | Application | 10/02/2008 15:02 |
| MyVolume | 665,600 KB | SES File | 10/02/2008 15:04 |

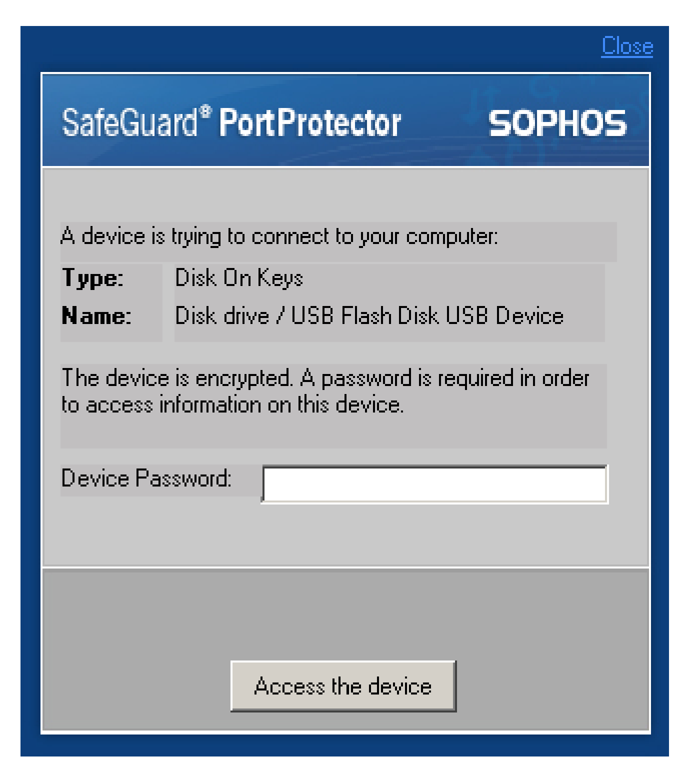
**Hinweis:** Löschen Sie den Container der verschlüsselten Dateien nicht vom Wechselspeichergerät. Durch das Löschen des Containers werden alle darin gespeicherten Daten gelöscht.

2 Doppelklicken Sie auf **AcessSecureData.exe**, um das Programm auszuführen und den Zugriff auf die Daten zu ermöglichen.

3 Das Hilfsprogramm wird ausgeführt und fordert das Kennwort für den Offline-Zugriff (das Kennwort, das in *Festlegen eines Kennworts für den Offline-Zugriff* festgelegt wurde) an, wenn ein verschlüsseltes Gerät zum ersten Mal an den Computer angeschlossen wird.

Was Sie sehen werden hängt davon ab, ob Sie über Administratorrechte verfügen oder nicht.

- **Administrator:** Geben Sie Ihr Kennwort ein und klicken Sie auf **Auf das Gerät zugreifen**.




Ein gemountetes Volume mit den verschlüsselten Daten wird angezeigt.

- **Non-Administrator:** Geben Sie Ihr Kennwort ein und klicken Sie auf **OK**.




Die *.ses-Datei (verschlüsseltes Volume) wird sich als ein Ordner mit den verschlüsselten Dateien öffnen. Um die Dateien zu benutzen, kopieren Sie sie auf den Schreibtisch des Computers. Wenn Sie fertig sind, kopieren Sie sie wieder auf das Gerät zurück.

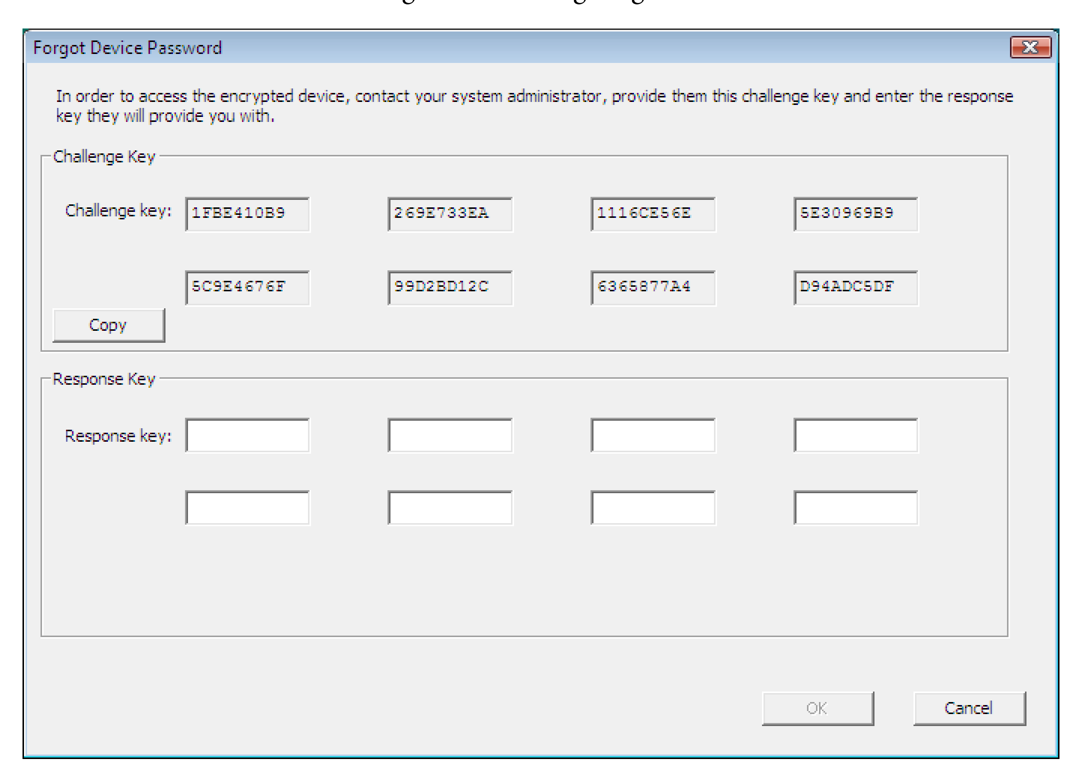
#### 8.7.3.3 Schlüssel für den Offline-Zugriff auf Geräte gewähren

**Hinweis:**

1. Dieses Verfahren ist nur für Geräte anwendbar, die durch die Volumen-Verschlüsselungsmethode verschlüsselt wurden.
2. Ein Endbenutzer benötigt Administrator-Rechte, um diesen Vorgang auf einem Computer auszuführen, auf dem Safend Protector nicht läuft

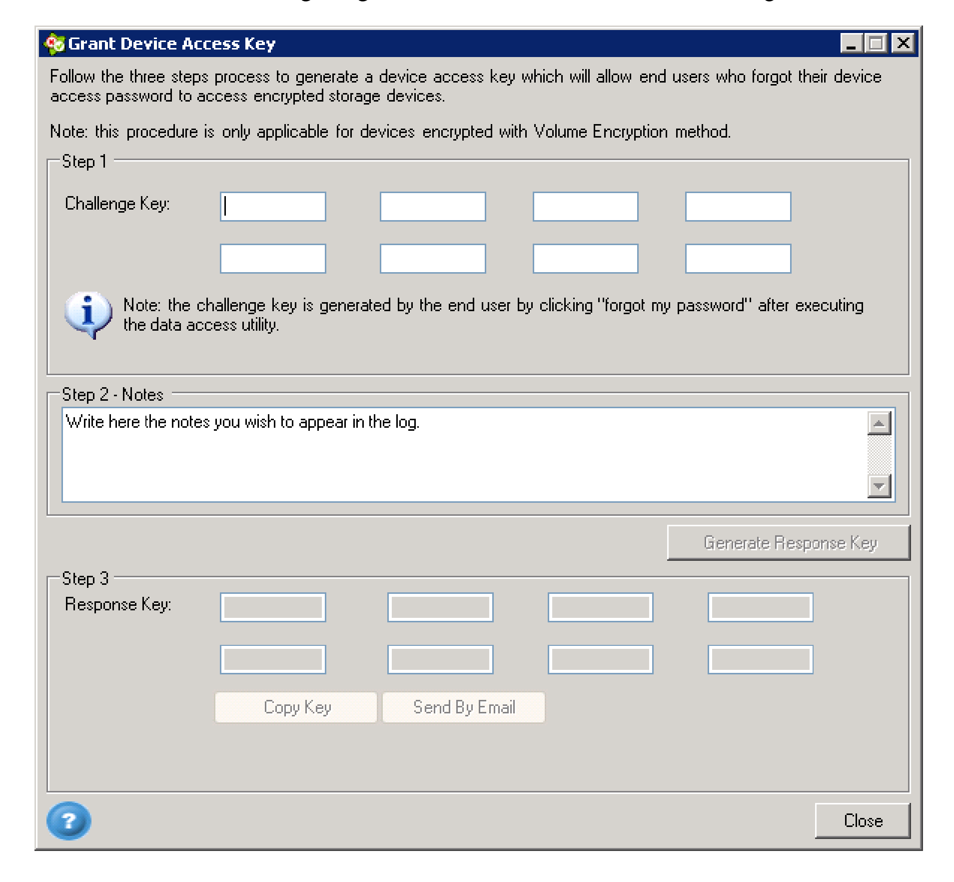
Das Utility Schlüssel für Gerätezugriff gewähren ermöglicht es einem Endbenutzer, der s ein Kennwort vergessen hat, auf ein verschlüsseltes Wechselspeichergerät (z. B. Disk-On-Key) auf einem Computer zuzugreifen, auf dem Safend Protector nicht läuft.

Der Endbenutzer klickt dann beim Zugriff auf das Datenzugriffstool auf Kennwort vergessen. Das Fenster Gerätekennwort vergessen wird angezeigt.




Senden Sie dem Administrator diesen Aufforderungsschlüssel (z. B. per E-Mail), und geben Sie den Antwortschlüssel ein, den Sie daraufhin erhalten haben. Klicken Sie auf die Schaltfläche OK. Sie haben jetzt Zugriff auf dieses Gerät.

Der Administrator greift auf diese Option von der Management Console aus zu. Klicken Sie auf **Schlüssel für Gerätezugriff gewähren** im Menü Extras. Das folgende Fenster wird angezeigt:



Es enthält die folgenden Schritte:

- **Schritt 1: Aufforderungsschlüssel**: Dies sind die Zahlen, die der Endbenutzer dem Administrator liefert (z. B. per E-Mail oder Telefon). Bei jedem Eingabefeld werden die Zeichen am Ende einer jeden Eingabesequenz überprüft. Wenn die Sequenz korrekt ist, wird das Zeichen ✓ rechts neben dem jeweiligen Eingabefeld angezeigt (und das Eingabezeichen wird zum nächsten Feld vorgeschoben). Wenn die Sequenz falsch ist, wird das Zeichen ✕ angezeigt *und es erscheint ein Hinweis.* "*Anmerkung: Falscher Aufforderungsschlüssel eingegeben. Bitte Aufforderungscode neu eingeben.*"
- **Schritt 2: Anmerkungen:** Dies wird aktiviert, nachdem der richtige Aufforderungsschlüssel eingegeben wurde. Geben Sie eine beliebige Anmerkung ein, die im Log erscheinen soll. Klicken Sie auf **Antwortschlüssel generieren**, um eine Antwort zu generieren.
- **Schritt 3: Antwortschlüssel:** Hierbei handelt es sich um Zahlen, die der Endbenutzer eingibt, nachdem er sie vom Administrator erhalten hat. Es werden bei richtiger bzw. falscher Eingabe von Zeichen dieselben Symbole wie für den Aufforderungsschlüssel angezeigt. Die Schaltfläche **Schlüssel kopieren** ermöglicht es Ihnen, den Antwortschlüssel zu kopieren (z. B. in Notepad), um ihn später zu verwenden. Mit der Schaltfläche **Per E-Mail senden** öffnen Sie eine neue E-Mail-Nachricht, die den Antwortschlüssel enthält.

Durch Klicken auf die Schaltfläche **Schließen** wird das Fenster geschlossen.

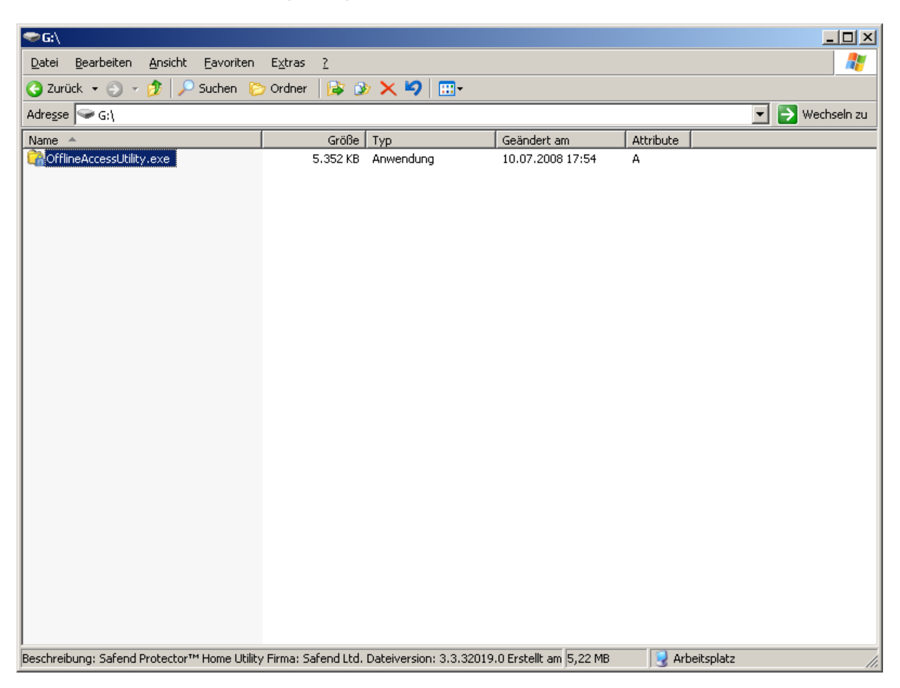
#### 8.7.3.4 Offline-Zugriff auf partitionsverschlüsselte Geräte

**Hinweis:** Für eine Beschreibung des Offline-Zugriffs bei ausgewählter Partitionsverschlüsselung siehe *Offline-Zugriff auf partitionsverschlüsselte Geräte.*

Wenn es die Policy des Endpunkts zulässt, kann der Endbenutzer auf organisatorisch verschlüsselte Geräte auf firmenfremden Computern mit Hilfe des von ihm festgelegten Kennworts für den Offline-Zugriff (Entschlüsselung) zugreifen. Bis der Endbenutzer das Kennwort eingegeben hat, kann nur auf das Offline Access Utility auf dem Gerät zugegriffen werden, welches das Dienstprogramm zur Eingabe des Kennworts ist.

**So greifen Sie offline auf ein partitionsverschlüsseltes Gerät zu (auf ungeschütztem Computer):**

1 Schließen Sie das verschlüsselte Gerät (für das ein Kennwort für den Offline-Zugriff festgelegt wurde) an den ungeschützten Computer an. Das folgende Windows-Fenster Mein Computer wird angezeigt:




**Hinweis:** Löschen Sie den Container der verschlüsselten Dateien nicht vom Wechselspeichergerät.

2 Doppelklicken Sie im Windows-Fenster Mein Computer auf **OfflineAccessUtility.exe**, um das Utility auszuführen. Das folgende Fenster wird angezeigt:




3 Das Hilfsprogramm wird ausgeführt und fordert das Kennwort für den Offline-Zugriff (das Kennwort, das in *Festlegen eines Kennworts für den Offline-Zugriff* festgelegt wurde) immer dann an, wenn ein verschlüsseltes Gerät an den Computer angeschlossen wird.

4 Klicken Sie auf **Verkleinern**, wenn Sie das Fenster schließen möchten. Das folgende Fenster wird angezeigt:




5 Klicken Sie auf **OK**. Das Hilfsprogramm läuft jetzt im Hintergrund und fordert das Kennwort für den Offline-Zugriff (das Kennwort, das in *Festlegen eines Kennworts für den Offline-Zugriff* festgelegt wurde) jedes Mal an, wenn ein verschlüsseltes Gerät an den Computer angeschlossen wird.

Sobald das Offline Access Utility läuft, wechselt das Offline Access Utility-Taskleistensymbol zu sobald Sie ein verschlüsseltes Gerät anschließen. Das folgende Fenster öffnet sich aus der Taskleiste:

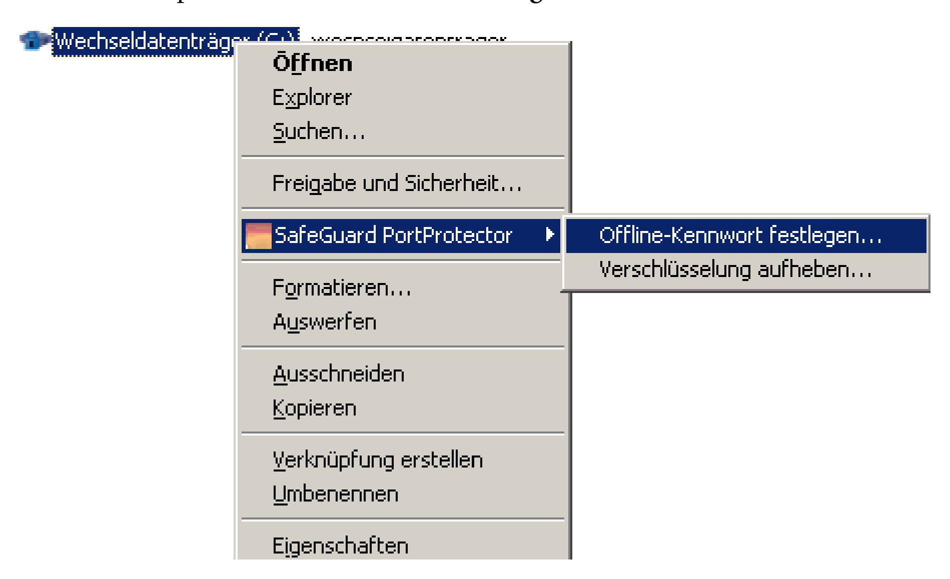



Dieses Fenster bleibt zwei Minuten lang geöffnet. In dieser Zeit können Sie das Entschlüsselungskennwort des Geräts eingeben. Nach Ablauf dieses Zeitraums wird das Fenster geschlossen, und Sie müssen es wieder öffnen, um das Gerät wieder anzuschließen. Solange Sie das Entschlüsselungskennwort nicht eingegeben haben, kann auf das verschlüsselte Gerät ist zugegriffen werden.

**So geben Sie ein Kennwort für den Offline-Zugriff ein:**

Geben Sie im Taskleistenfenster das *Gerätekennwort* ein und klicken Sie auf **Auf das Gerät zugreifen**. Auf die Daten auf dem Gerät kann jetzt zugegriffen werden, und das Taskleistensymbol ändert sich zu **Verschlüsselt** .

**Hinweis:** Wenn das Fenster *Offline Access Password* verschwindet, bevor Sie das Kennwort eingeben konnten, geben Sie das Kennwort ein, indem Sie mit der rechten Maustaste in Mein Computer auf das Gerät klicken und die Shell-Erweiterung **SafeGuard PortProtector** wählen, in der sich die Option **Offline-Kennwort festlegen** befindet.




**Hinweis:** Wenn Sie das Gerät entfernen, müssen Sie das Entschlüsselungskennwort wieder eingebeben, sobald Sie es das nächste Mal anschließen. Die Wiederholversuche für die Eingabe des Kennworts sind limitiert, um unrechtmäßigen Zugang zu verhindern. Wenn Sie diese Grenze überschreiten müssen Sie das Gerät an einen Computer anschließen, auf dem SafeGuard PortProtector läuft, um auf das Gerät zuzugreifen.

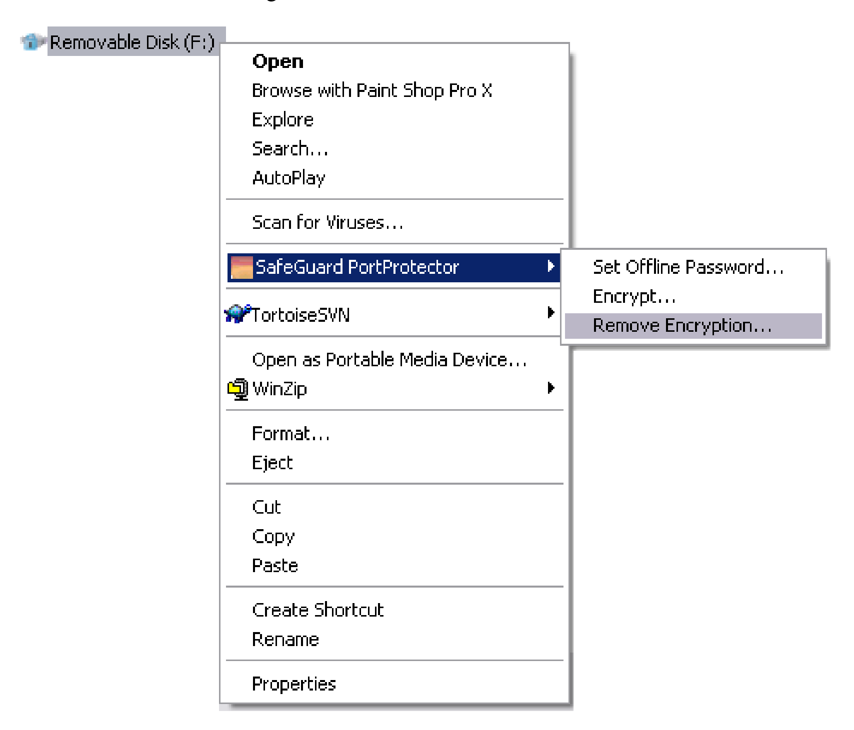
### 8.7.4 Entfernen der Verschlüsselung

Sie können bei Bedarf die Verschlüsselung von verschlüsselten Geräten entfernen. Dies wird nicht empfohlen, wenn es nicht unbedingt erforderlich ist, da die Daten auf Ihrem Gerät verloren gehen und das Gerät nicht mehr geschützt ist.

**So entfernen Sie die Verschlüsselung:**

1 Schließen Sie das Gerät an.

2 Klicken Sie in Mein Computer mit der rechten Maustaste auf das Gerät, und wählen Sie die Shell-Erweiterung SafeGuard PortProtector.




3 Wählen Sie **Verschlüsselung entfernen**. Das folgende Fenster wird angezeigt:



**Hinweis:** Beim Entfernen der Verschlüsselung wird das Gerät formatiert. Das bedeutet, dass alle Daten auf dem Gerät gelöscht werden. Es wird dringend empfohlen, dass Sie die Daten sichern, bevor Sie die Verschlüsselung entfernen.

4 Klicken Sie auf **Weiter**. Das folgende Bestätigungsfenster wird angezeigt:




5 Klicken Sie auf **OK**, um mit der Entfernung der Verschlüsselung zu beginnen. Es wird eine Fortschrittsanzeige angezeigt. Sobald der Vorgang beendet ist, wird folgendes Fenster angezeigt:




6 Klicken Sie auf **Beenden**, um den Assistenten *Remove Encryption* zu beenden

**Hinweis für Systemadministratoren:** Endbenutzer mit einer gültigen Policy, die eine Verschlüsselung der Wechselspeichergeräte erfordert, müssen über die Anleitungen in *Verschlüsselung und Entschlüsselung von Wechselspeichergeräten* in *Kapitel 9, Endbenutzer-Erfahrung, im Benutzerhandbuch* informiert werden, da der Client möglicherweise Meldungen anzeigt, die sie zur Verschlüsselung der Wechselspeichergeräte auffordern. Benutzer, deren geltende Policy die Entschlüsselung und Heimnutzung verschlüsselter Speichergeräte ermöglicht, müssen darüber hinaus die Anleitungen in *Offline-Zugriff auf verschlüsselte Geräte* erhalten, damit Sie wissen, wie ein Kennwort für den Offline-Zugriff festgelegt und Geräte entschlüsselt werden.

### 8.7.5 Verfolgen der Offline-Nutzung verschlüsselter Geräte

Wenn autorisierte Endbenutzer verschlüsselte Wechselspeichergeräte auf organisationsfremden Computern benutzen, möchten Sie ggf. alle Dateiübertragungen rückverfolgen, die sie vom/zum Gerät durchgeführt haben. Mit SafeGuard PortProtector können Sie das (siehe *Schritt 10: Protokollierung definieren* in *Kapitel 3, Definieren von Policies).*

Wenn Sie diese Option aktivieren, werden alle Informationen zu Offline-Dateiübertragung auf dem verschlüsselten Gerät gespeichert. Sobald das verschlüsselte Gerät wieder an das Organisationsnetz angeschlossen wird, werden alle gespeicherten Logs an den Management Server gesendet und können unter File Logs in die Logs-Welt eingesehen werden.

## 8.8 CD/DVD-Verschlüsselung

Über die Safend Protector CD/DVD-Verschlüsselung können Endbenutzer Daten auf CD/DVD-Medien verschlüsseln. Verschlüsselte CD/DVDs werden mit Hilfe von Organisationsschlüsseln verschlüsselt. Das bedeutet, dass auf die darin enthaltenen Ordner und Dateien von jedem Computer der Organisation zugegriffen werden kann. Außerdem kann der Zugriff darauf auch mit Hilfe des Access Utility von einem ungeschützten Computer aus erfolgen.

### 8.8.1 Erstellen einer verschlüsselten CD/DVD

Safend Protector startet automatisch den Assistenten *Verschlüsselte Disk erstellen*, mit dem Sie ein verschlüsseltes Volume erzeugen können, wenn Sie eine unverschlüsselte CD/DVD auf einem geschützten Computer brennen wollen. Der Assistent wird auf einem der folgenden Wege gestartet:

Wenn ein Benutzer, der ein CD/DVD-Medium gemäß der Policy verschlüsseln muss, ein leeres beschreibbares Medium in einem geschützten Computer einlegt, wird ein Fenster angezeigt:

Klicken Sie auf **Verschlüsseln**, um die erste Seite des Assistenten *Verschlüsselte Disk erstellen* anzuzeigen, wie weiter unten in Schritt 3 beschrieben. Alternativ wird, wenn Sie mit der rechten Maustaste auf das Brenner-Laufwerk klicken, ein Menü angezeigt. Wählen Sie Safend Protector und dann Verschlüsselte CD/DVD erstellen, um die erste Seite des Assistenten 'Verschlüsselte Disk erstellen' anzuzeigen.

### 8.8.2 Erstellen und Verwenden einer verschlüsselten CD/DVD

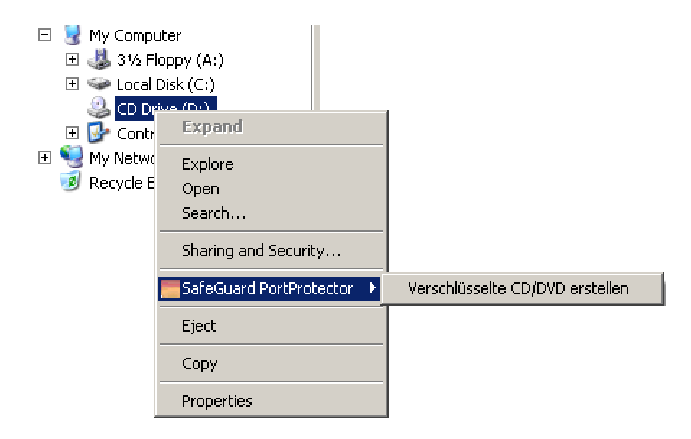
Mit dem Assistenten 'Verschlüsselte Disk erstellen' können Sie ein verschlüsseltes CD/DVD-Medium erstellen.

**So öffnen Sie den Assistenten 'Verschlüsseltes Volume erstellen':**

Sie können den Assistenten *Verschlüsselte Disk erstellen* auf zwei Arten öffnen:

1 Klicken Sie mit der rechten Maustaste auf ein CD/DVD-Laufwerk.

2 Wählen Sie **SafeGuard Protector** und dann **Verschlüsselte CD/DVD erstellen**:




3 Klicken Sie im *SafeGuard PortProtector Client*-Fenster – auf die Registerkarte **Tools.** Das folgende Fenster wird angezeigt:




4 Klicken Sie auf die Schaltfläche **Disk verschlüsseln.**
Der Assistent *Verschlüsselte Disk erstellen* wird angezeigt.

**So erstellen Sie eine verschlüsselte CD/DVD:**

Dieser Assistent führt Sie durch die Erstellung einer verschlüsselten CD/DVD.

1 Öffnen Sie den Assistenten *Verschlüsselte Disk erstellen* wie oben beschrieben. Der folgende Assistent wird angezeigt.




2 Geben Sie die *Größe der Disk*. Wählen Sie eine der Standardgröße für CD oder DVD, oder geben Sie eine Größe im Feld *Sonstige* ein. Klicken Sie auf **Next**.

3 Wenn Sie über die Berechtigung verfügen, ein Kennwort für den Zugriff auf Speichergeräte außerhalb der Organisation festzulegen, wird das folgende Fenster angezeigt.



Wählen Sie ein Kennwort, das auf Computern außerhalb Ihrer Organisation genutzt wird, um auf den Inhalt zuzugreifen. Sie ein Kennwort nur **vor dem Brennen** der CD/DVD festlegen.

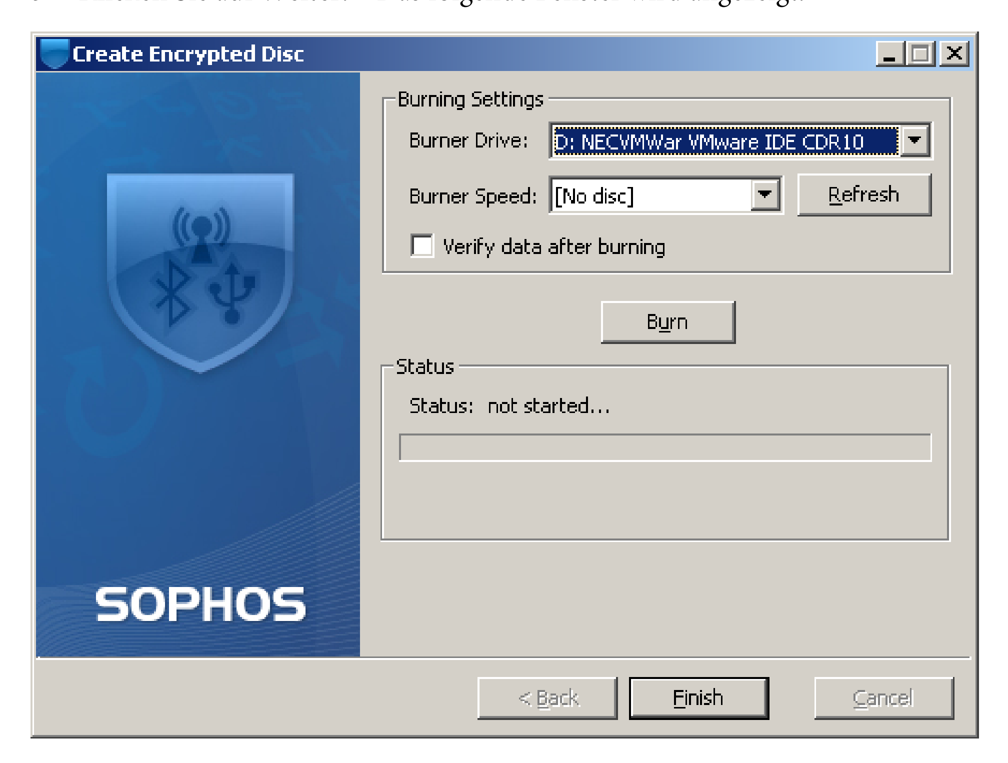
**Hinweis:** Das von Ihnen festgelegte Kennwort muss den Kennwortregeln in Ihrer Organisation entsprechen.

4 Klicken Sie auf **Weiter**. – Das folgende Fenster wird angezeigt:




Klicken Sie auf **Volume öffnen** und fügen Sie Dateien von Ihrem Computer zur verschlüsselten Disk hinzu.

5 Klicken Sie auf **Weiter**. – Das folgende Fenster wird angezeigt:



6 Wählen Sie das *Brenner-Laufwerk* und die *Brenner-Geschwindigkeit* für die CD. Klicken Sie auf **Aktualisieren**, um CD oder Brenner zu ändern. Wählen Sie *Daten nach dem Brennen überprüfen*, wenn Sie prüfen möchten, ob sich die Daten auf der Disk befinden.

7 Klicken Sie auf **Brennen**, um den Vorgang zu starten. Der Fortschritt wird im *Brennfortschritt* angezeigt.

Hinweis: Unter Windows 2000 ist das Verhalten anders. Wenden Sie sich an Safend, um weitere Informationen zu erhalten.

8 Klicken Sie auf **Finish**, um den Assistenten zu beenden.

### 8.8.3 Offline-Zugriff auf verschlüsselte CD/DVD

Der Zugriff auf eine verschlüsselte CD/DVD variiert abhängig davon, ob Sie Administratorrechte haben oder nicht.

# 9 Appendix A – Novell eDirectory Synchronization

## About This Appendix

Similarly to its existing seamless integration with Active Directory, SafeGuard PortProtector supports full integration with Novell's eDirectory. With this integration the Management Server can be configured to connect to the eDirectory in order to import the organizational tree, including OUs, Groups, Users and Computers. This enables viewing of directory objects (computers/user groups) through the Management Console for policy association, log filtering and Client management purposes.

When you configure a SafeGuard PortProtector system to synchronize with eDirectory, you will typically choose to distribute policies using the Policy Server (see *Verteilen von SafeGuard PortProtector Policies direkt vom* Management Server aus in *Chapter Distributing Policies*). However, if you wish to use a different distribution method, such as a third party tool using registry files, you can do so. To learn about policy distribution methods refer to *Chapter Verteilen von* Policies.

## 9.1 Configuring SafeGuard PortProtector to Synchronize with Novell eDirectory

Configuring SafeGuard PortProtector to synchronize with Novell eDirectory is performed in the *Administration* window and explained below (refer to *Chapter* **Error! Reference source not found.** for further details about the *Administration* window).

**Note:** There is no need for a Novell client to be installed on the SafeGuard PortProtector Management Server machine.

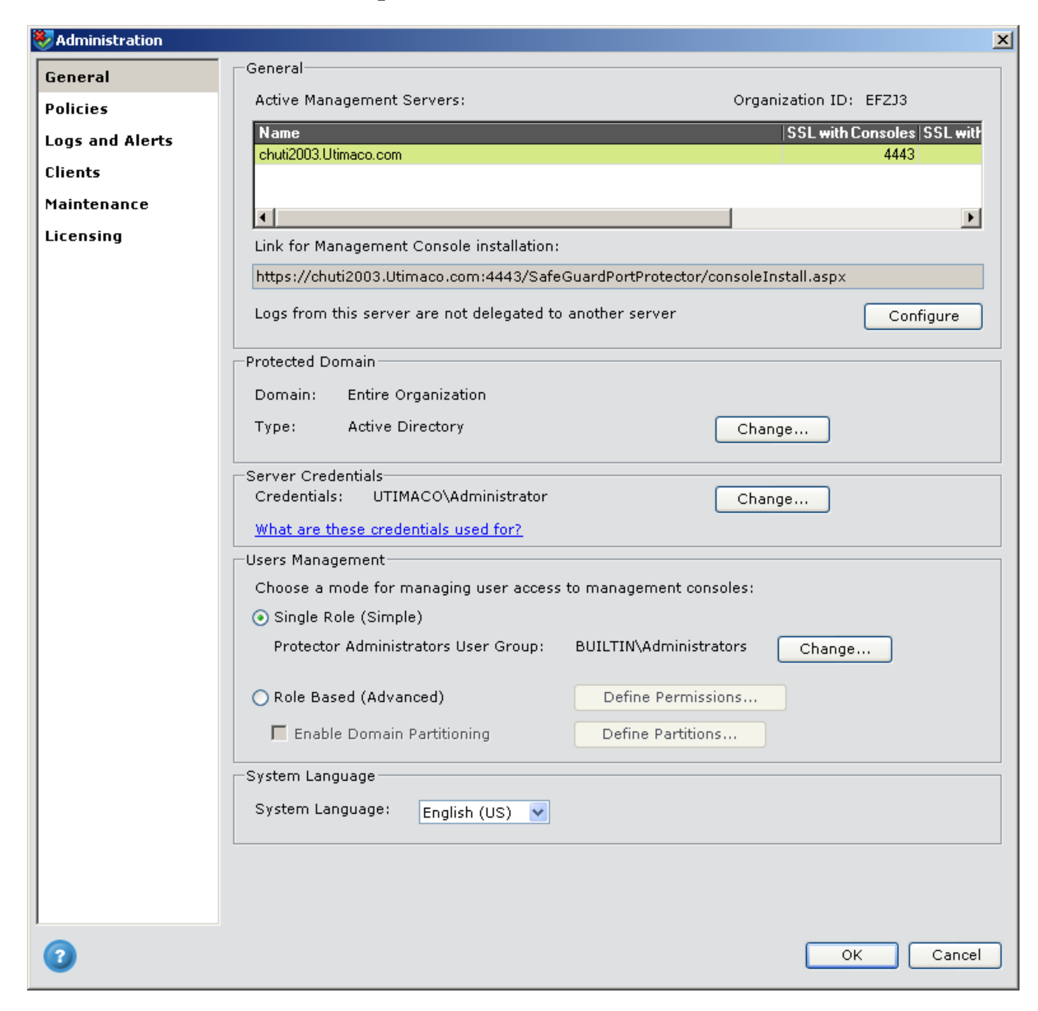
**To open the *Administration* window:**

From the *Tools* menu, select **Administration**

OR

In the Home World, from the *More* section, click the **Change Administration Settings** link.

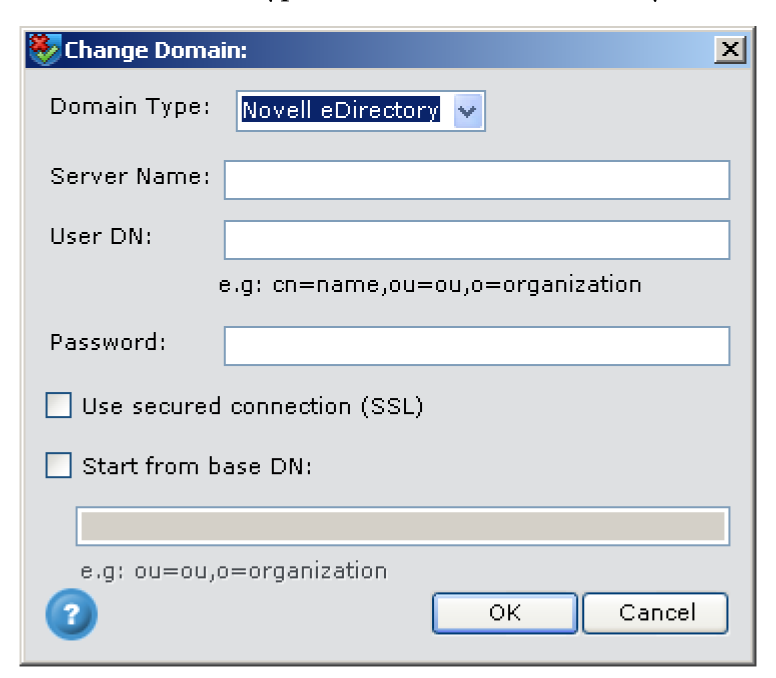
The *Administration* window opens:




The default Directory setting is an Active Directory. To synchronize with Novell eDirectory instead, you need to change this setting.

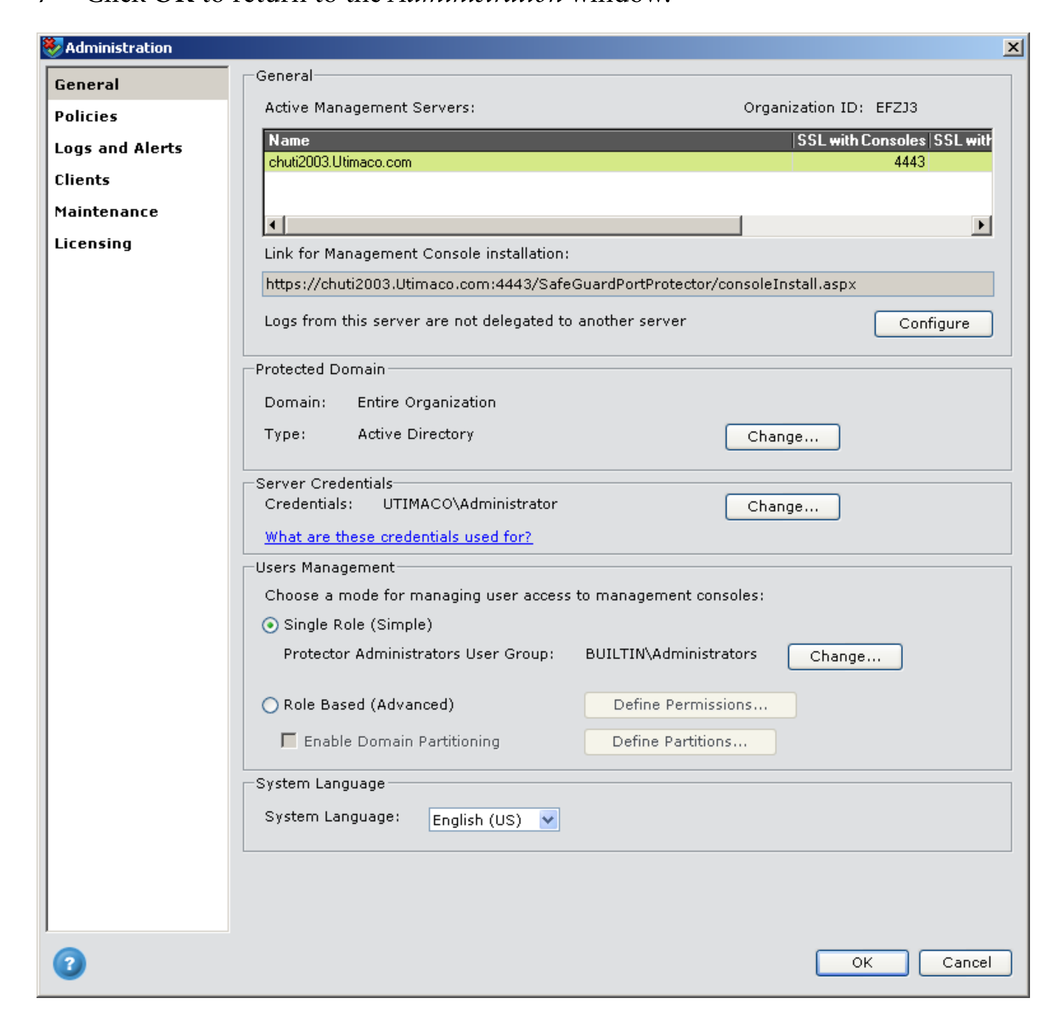
**To change Directory setting:**

1. In *General* page, in the **Protected Domain** section, click **Change.** The *Change Domain* window opens:
2. In the **Domain Type** field, select **Novell eDirectory** from the drop-down menu.




3. In the **Server Name** field, enter the Novell server name.
4. In the User DN field, enter the user information. This user should have reading privileges for all Novell objects. The format is cn=name,ou=ou,o=organization.
5. In the Password fields enter the user's password.
6. If you want to protect starting from a specific DN, in order to protect a specific branch or office and not the entire organization, check the Start from Base DN checkbox and enter the DN. If you want to apply protection to the entire organization, leave the checkbox unchecked.

7 Click **OK** to return to the *Administration* window:




8 In the *Administration* window, click **OK**.

SafeGuard PortProtector will now be synchronized with eDirectory. All previous tree objects are deleted.

**Note:** When using Novell, it is best to perform the above configuration prior to installing Clients. This way, the Client installation will contain the appropriate configuration and Clients will immediately identify themselves as Novell clients.

**Note:** If you previously had policies applied to deleted AD tree objects, you can still view their logs through querying logs by name.

## 9.2 A Few Additional Points

- When using Novell, role-based administration (explained in Role Based (Advanced)in *Chapter 7, Administration*) is possible only using local groups on the Management Server.
- SafeGuard PortProtector Client detects changes in the Novell user logged in to the endpoint using login and changes the effective endpoint policy accordingly. In-session user changes are not detected. This means that the previous user's policy remains effective until it is either updated from the *Client* window (see *Aktualisieren der Client-Policy* in *Chapter 9, End-user Experience*) or until the next update occurs according to the policy update interval.
- In logs, Novell objects appear in type-less format (for example mike.pm.acme.com)

# 10 Appendix B - Supported Device Types

## About This Appendix

This appendix lists the device types that SafeGuard PortProtector provides for your selection when building a policy.

For **non-storage devices** you can restrict the usage of devices on USB, FireWire and PCMCIA ports. SafeGuard PortProtector provides a selection of built-in types in the *Device Control* window to enable you to define which types of devices are approved or blocked. If you require control of a device type that is not listed here, you can use the Distinct Device restriction feature described in *Approving Devices and WiFi Connections* in *Chapter 3, Defining Policies*.

For **storage devices**, SafeGuard PortAuditor is able in most cases to identify whether a device is a storage device or a non-storage device, by detecting its volume, or using its embedded class data. This ability helps categorize and organize device lists into storage devices and simple (non-storage) devices for your selection, thus enabling you to define your policy more easily. SafeGuard PortProtector provides a selection of built-in types in the *Storage Control* window to enable you to define which types of devices will be approved or blocked, as described in *Chapter 3, Definieren von* Policies.

The following device type lists are divided into Non-Storage Devices and Storage Devices.

## 10.1 Non-Storage Device Types

The following lists the non-storage built-in device types for which a policy can be defined in SafeGuard PortProtector.

**Note:** Device Control for non-storage devices can only be defined for USB, FireWire and PCMCIA ports.

Human Interface Device - devices used to control the operation of computer systems. Typical examples include keyboards and pointing devices, such as: mouse, trackballs and joysticks.

**Printing Devices –** Printers connected over USB, PCMCIA or FireWire

Personal Data Assistants (PDA's) - These include:

- Windows Mobile / Pocket PC Devices
- Blackberry Devices
- Palm OS Devices

**Mobile Phones –** New models of cellular phones, categorized in USB as 'Wireless USB Devices'

**Network Adapters** - Communication devices such as: Ethernet network adapters, WiFi adapters and USB-connected ADSL and cable modems.

**Imaging Devices** - Primarily devices such as scanners and digital still cameras.

**Audio/Video Devices** - devices such as: microphones, telephones, volume controls, web cameras, digital camcorders, digital television tuners and digital still-image cameras that support video streaming.

**Smart Cards** - Smart Card devices.

**Content Security Devices** - used to provide special security features, such as strong authentication, biometric identification and software licensing.

## 10.2 Storage Device Types

Protection of storage devices applies to all non-blocked ports, meaning that it applies to the specified storage device no matter to which port it is connected as long as that port is not defined as blocked.

**Note:** Device Control for storage devices can be defined for any port type including, for example, parallel ports, USB, FireWire and PCMCIA ports.

Internally attached storage device are also controlled

The following lists the storage built-in device types that are supported by SafeGuard PortProtector.

**Removable storage devices** - These devices range from storage-only devices, such as disk-on-key, Memory Sticks and SD flash cards, to devices that have a unique purpose, but appear to the computer as a new storage drive, such as portable digital music players, digital cameras and PDAs.

**External Hard Disks –** hard disk devices which are externally attached (e.g. via USB)

**CD/DVD Drives –** both internally and externally attached

**Floppy Drives** - both internally and externally attached

Tape Drives - both internally and externally attached

# 11 Appendix C – Supported File Types

## About This Appendix

The following table lists the file types and extensions supported by SafeGuard PortProtector's File Type Control.

| File Type | Extensions | Description |
|---|---|---|
| **Microsoft Office** | DOC | Microsoft Word Document |
| | DOCX | Microsoft Word Document |
| | DOCM | Microsoft Word Document |
| | DOT | Microsoft Word Template |
| | DOTX | Microsoft Word Template |
| | DOTM | Microsoft Word Template |
| | RTF | Rich Text Format |
| | PPT | Microsoft PowerPoint Presentation |
| | PPTX | Microsoft PowerPoint Presentation |
| | PPTM | Microsoft PowerPoint Presentation |
| | POT | Microsoft PowerPoint Template |
| | POTX | Microsoft PowerPoint Template |
| | POTM | Microsoft PowerPoint Template |
| | PPS | Microsoft PowerPoint Show |
| | PPSX | Microsoft PowerPoint Show |
| | PPSM | Microsoft PowerPoint Show |
| | PPA | Microsoft PowerPoint Add-In |
| | PPAM | Microsoft PowerPoint Add-In |
| | XLS | Microsoft Excel Workbook |
| | XLSX | Microsoft Excel Workbook |
| | XLSM | Microsoft Excel Workbook |
| | XLSB | Microsoft Excel Workbook |
| | XLT | Microsoft Excel Template |
| | XLTX | Microsoft Excel Template |
| | XLTM | Microsoft Excel Template |
| | XLA | Microsoft Excel Add-In |
| | XLAM | Microsoft Excel Add-In |
| | MPP | Microsoft Project Project |

| File Type | Extensions | Description |
|---|---|---|
| | MPT | Microsoft Project Template |
| | VSD | Microsoft Visio Drawing |
| | VDX | Microsoft Visio Drawing |
| | VSS | Microsoft Visio Stencil |
| | VSX | Microsoft Visio Stencil |
| | VST | Microsoft Visio Template |
| | VTX | Microsoft Visio Template |
| | PUB | Microsoft Publisher |
| | ONE | Microsoft OneNote Sections |
| | ADP | Microsoft Access Project |
| | ADE | Microsoft Access Project Extension |
| **Published Documents** | PDF | Adobe Acrobat Document |
| | PS | Post Script Document |
| | EPS | Encapsulated Post Script |
| **Web Pages** | HTML | HTML Web Page |
| | HTM | HTML Web Page |
| | MHT | Archived Web Page |
| | MHTML | Archived Web Page |
| | PHP | PHP Script |
| | HLP | Windows Help File |
| | CHM | Compiled Help File |
| | ASP | Active Server Page |
| | ASPX | ASP.NET Web Page |
| | ASMX | ASP.NET Webservices |
| | JHTML | Java HTML Web Page |
| | JSP | Java Server Page |
| **Images** | JPG | JPEG Image |
| | JPEG | JPEG Image |
| | GIF | GIF Image |
| | BMP | Bitmap Image |
| | DIB | Device Independent Bitmap Image |
| | PNG | PNG Image |
| | TIF | Tagged Image Format |
| | TIFF | Tagged Image Format |
| | MDI | Office Document Imaging File |
| | JNG | JNG Image |
| | MNG | MNG Image |

| File Type | Extensions | Description |
|---|---|---|
| | ICO | Windows Icon |
| | CUR | Windows Cursor |
| | WMF | Windows Metafile Image |
| | EMF | Enhanced Windows Metafile Image |
| | FH9 | Macromedia Freehand 9 Graphics |
| | JP2 | JPEG-2000 Image |
| | PBM | Portable Bitmap |
| | PGM | Portable Graymap Bitmap |
| | PPM | Portable Pixelmap Bitmap |
| | PSD | Adobe Photoshop Graphics |
| | CDR | CorelDRAW Vector Graphics |
| | SVG | Scalable Vector Graphics |
| **Multimedia** | WAV | Waveform Audio |
| | WMA | Windows Media Audio |
| | MP2 | MPEG Audio |
| | MP3 | MPEG Audio |
| | AIFF | Audio Interchange |
| | AIF | Audio Interchange |
| | AU | AU Audio |
| | RA | RealMedia Streaming Media |
| | MID | Musical Instrument Digital Sound |
| | MIDI | Musical Instrument Digital Sound |
| | RMI | Musical Instrument Digital Sound |
| | SDS | Musical Instrument Digital Sound Sample |
| | VOC | Creative Lab's Soundblaster Audio |
| | OGG | Ogg Vorbis Codec Audio |
| | VOX | Dialogic Audio |
| | FLAC | Free Loseless Codec Audio |
| | MPEG | MPEG Multimedia |
| | MPG | MPEG Multimedia |
| | AVI | Audio Video Interleave |
| | ASF | Advanced Streaming Format |
| | WMV | Windows Media Multimedia |
| | MOV | QuickTime Video Clip |
| | SWF | Flash Animation File |
| | FLI | FLIC Animation |
| | FLC | FLIC Animation |

| File Type | Extensions | Description |
|---|---|---|
| **Text & Program Code** | TXT | Text File |
| | CSV | Formatted Text (Comma Delimited) |
| | PRN | Formatted Text (Space Delimited) |
| | CPP | C++ Program Code |
| | C | C/C++ Program Code |
| | H | C/Java Header File |
| | XML | XML File |
| | F | FORTRAN Program Code |
| | T90 | FORTRAN Program Code |
| | MAKEFILE | Compilation Control File |
| | MAKEFILE.IN | Compilation Control File |
| | PL1 | PL1 Program Code |
| | ASM | Assembler Progeam Code |
| | PAS | PASCAL Program Code |
| | JAVA | JAVA Program Code |
| | M4 | Meta4 Program Code |
| | BCPL | BCPL Program Code |
| | CS | Visual C#.NET Program Code |
| | PL | Perl Program Code |
| | PM | Perl Program Code Module |
| | PY | Python Program Code |
| | PDB | Visual C++/.NET Program Database |
| | BAS | BASIC Program Code |
| | VB | Visual Basic Program Code |
| | VBS | VBScript Script |
| | JS | JavaScript Source Code |
| **Executables** | EXE | Executable |
| | DLL | Dynamic Link Library |
| | PIF | Windows Program Information File |
| | BAT | Batch |
| | COM | Command |
| | OCX | ActiveX - Object Linking and Embedding (OLE) Control Extension |
| | CMD | Command |
| | CPL | Windows Control Panel Extension |
| | SCR | Windows Screen Saver |
| | VXD | Virtual Device Driver |
| | SYS | System Device Driver |

| File Type | Extensions | Description |
|---|---|---|
| | CLASS | Java Bytcode |
| | PYC | Python Compiler Script (Bytecode) |
| | LIB | Program Library Common Object File Format (COFF) |
| | INS | InstallShield Script |
| | OBJ | Object File |
| | O | Object File |
| **Compressed Archives** | ZIP | ZIP Compressed Archive |
| | ARJ | ARJ Compressed Archive |
| | RAR | WinRAR Compressed Archive |
| | GZIP | GZIP Compressed Archive |
| | TAR | Tape Archive |
| | JAR | JAR Compressed Archive |
| | ACE | WinAce Compressed Archive |
| | HQX | Macintosh BinHex 4 Compressed Archive |
| | LZH | LHA Compressed Archive |
| | LHA | LHA Compressed Archive |
| | AR | AIX Small Indexed Archive |
| | ARC | LH ARC Compressed Archive |
| | CAB | Cabinet Compressed Archive |
| | **_ | Compressed Installation Files (e.g. EX_, DL_) |
| **CD/DVD Disc Images** | ISO | ISO Disc Image |
| | BIN | BIN Disc Image |
| | CIF | EasyCD Creator Disc Image |
| | CCD | CloneCD Disc Image |
| | IMG | CloneCD Disc Image |
| | MDF | Alcohol 120% Disc Image |
| | DAA | PowerISO Disc Image |
| | C2D | WinOnCD Disc Image |
| **Databases** | MDB | Microsoft Access Database |
| | ACCDB | Microsoft Access Database |
| | ACCDT | Microsoft Access Database Template |
| | MDA | Microsoft Access Add-In |
| | MDW | Microsoft Access Workgroup |
| | MDE | Microsoft Access Compiled Database |
| | MYD | MySQL MyISAM Database |
| | MYI | MySQL MyISAM Database Index |

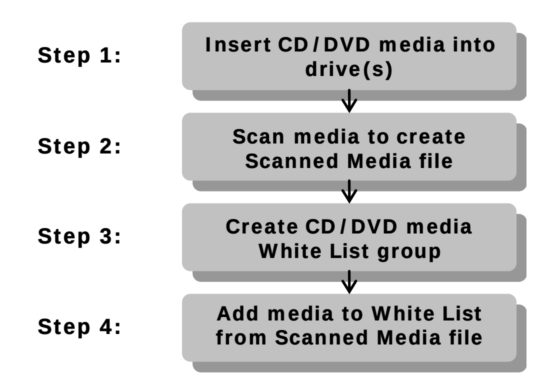
| File Type | Extensions | Description |
|---|---|---|
| | FRM | MySQL MyISAM Generic Dictionary |
| | DBF | dBase Database |
| | DBT | Microsoft FoxPro Database |
| | GDB | Borland InterBase Database |
| | PX | Paradox Database |
| **Microsoft Outlook** | PST | Outlook Personal Folder |
| | DBX | Outlook Express E-mail Folder |
| **PGP Encryption** | PGP | Pretty Good Privacy (PGP) Encrypted |
| | ASC | Pretty Good Privacy (PGP) Armored Encrypted |
| | CTX | Pretty Good Privacy (PGP) Ciphertext |
| **Computer-Aided Design (CAD)** | DWG | AutoCAD Drawing |
| | DXF | AutoCAD Interchange |
| | ASM | Pro/ENGINEER Assembly |
| | PRT | Pro/ENGINEER Model |
| **Adobe FrameMaker** | DOC | Adobe FrameMaker/FrameBuilder Document |
| | FM | Adobe FrameMaker Document |
| | FRM | Adobe FrameMaker Document |
| | BOOK | Adobe FrameMaker Book |
| | MIF | Adobe FrameMaker Interchange Format |

# 12 Appendix D – CD/DVD Media Scanner

## About This Appendix

In addition to controlling CD/DVD drives, SafeGuard PortProtector includes the ability to identify specific CD/DVD media, in order to authorize their use. A special scanning mechanism known as the Media Scanner computes a unique "fingerprint" identifying the data on each medium, and adds the medium's details to its output file (the Scanned Media file). The Media Scanner may be used on any computer and does not require any network connection to the Management Server. This allows you to run the utility on a stand-alone machine in order to avoid the inherent risks of viruses and Trojans which can be introduced via CDs and DVDs.

From the output file, scanned media can then be added to a CD/DVD Media White List in order to authorize their use. This means that any medium that is not white-listed is prohibited, unless it is used through a specific, white-listed CD/DVD drive (CD/DVD media and device white lists are explained in detail in *Chapter 3, Definieren von* Policies.) Any change made to the data on the medium following the scan will revoke its fingerprint, and in turn make it unapproved. The process of fingerprinting media and adding them to the CD/DVD Media White List is summarized in the following chart:




The process of creating a CD/DVD media White List (steps 3 and 4) is explained in *Freigeben von CD/DVD-Medien* in *Chapter 3, Defining Policies.*

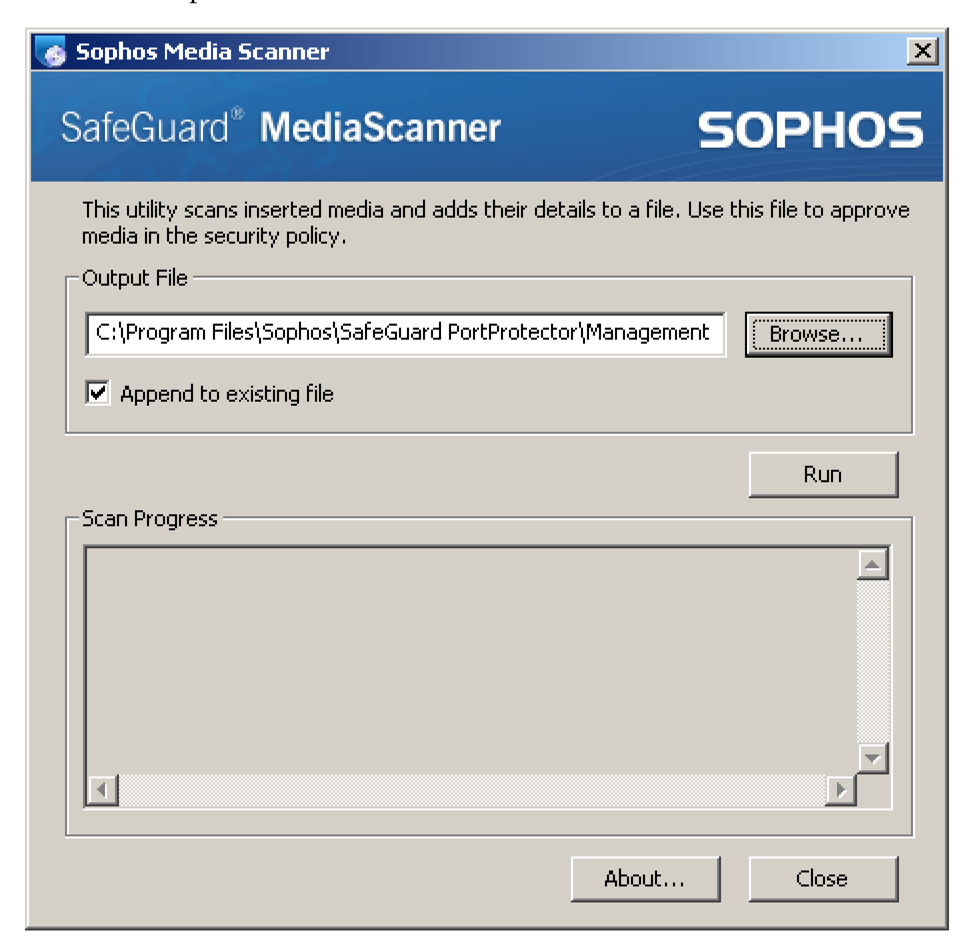
## 12.1 Scanning and Fingerprinting Media

Before a CD/DVD medium can be authorized by adding it to a CD/DVD Media White List, it must be scanned in order to "fingerprint" it and add the fingerprinted medium's details to an output file (referred to below as the Scanned Media file). This is performed using the Media Scanner, provided with the installation package. The Media Scanner can be run on any computer.

**Note:** Audio CDs are not supported by the Media Scanner. If you attempt to scan an audio CD the scan will fail.

**To scan a CD/DVD and add it to the scanned media file:**

1 On the SafeGuard PortProtector Management Server machine run `MediaScanner.exe` from `\Program Files\Utimaco\SafeGuard PortProtector\Management Server\tools`, or copy `MediaScanner.exe` to any computer and run it. The following window opens:




2 If you wish to change the default output file name or location, use the Browse button.

**Note:** If you change the file name, the suffix must remain .XML.

3 By default, the Media Scanner is set to append scanned media information to the existing scanned media file. If you wish to add media to a new file, uncheck the **Append to existing file** checkbox.

4 Insert the required media into the CD/DVD drives and click Run. The scanning process begins.

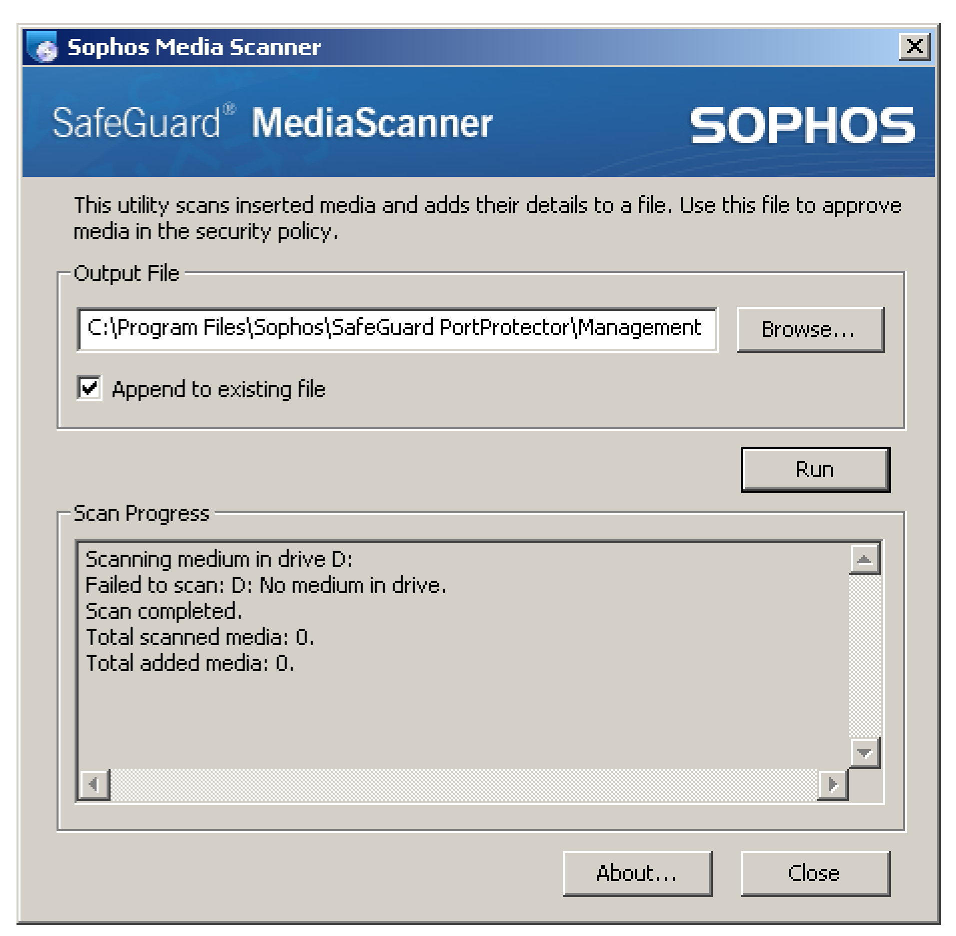
**Note:** The process scans all media inserted into CD/DVD drives at the time of the scan, meaning you may scan more than one medium in each session.

5 You can view the scan progress in the **Scan Progress** section, which includes the following details:

- **Drive**: name of the drive in which scanned medium is inserted
- **Volume Name**: name of the scanned volume, if one has been assigned
- **Type**: CD or DVD
- **Fingerprint**: a readable version of the fingerprint
- **Size**: size of the content on the medium
- **Time**: date and time when scan was performed

**Note:** If the Scanned media file contains more than one medium, and the volume name is non-existent or is not sufficient in order for you to identify the medium later when adding media to the White List, make sure other details provided in the Scan Progress section are available to you when adding media to the White List (refer to *Freigeben von CD/DVD-Medien* in *Chapter 3, Defining Policies*). You can also view these details in the scanned Media file, as explained in *Viewing the Scanned Media File* below.

Once a scan is completed, the Scan Progress section displays the total of scanned media and the total number of media added to the Scanned Media file, as shown in the following figure.




**Note:** If a scan fails, a notification appears in the Scan Progress section.

Upon completion of a scan, you may repeat the process for additional media by inserting a medium into the CD/DVD drive and clicking Run.

## 12.2 Viewing the Scanned Media File

If you wish, you may open the Scanned Media file in order to view scan details.

**To view the scanned media file contents:**

Open the file using Microsoft Excel. The file contains one line for each medium, and displays the following columns:

- **VolumeName**: name of the scanned volume, if one has been assigned
- **Type**: CD or DVD
- **Size**: size of the content on the medium
- **Time**: date and time when scan was performed
- **ShortFingerprint**: a shorter version of the long fingerprint
- **LongFingerprint**: the actual fingerprint used by SafeGuard PortProtector

**Note**: When viewing the file, do not make any changes to it. Modifying the file may later prevent adding the modified medium to the CD/DVD Media White List.

# 13 Appendix E - Using SafeGuard PortProtector in a HIPAA Regulated Organization

## About This Appendix

Recent security breaches and changes in the use of portable and storage technology have prompted the Department of Health and Human Services (DHHS) to require Health Insurance Portability and Accountability Act (HIPAA) regulated organization's (i.e., covered entities) to address data leakage problems. In recognition of the data leakage threat, DHHS has issued specific guidance for the use of portable mobile devices and offsite transport of EPHI such as laptops, PDAs, and USB drives (HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information, Department of Health & Human Services, Centers for Medicare & Medicaid Services, January 8, 2007).

The Privacy and Security Rules of HIPAA requires regulated organizations to protect Electronic Protected Health Information (EPHI). These security rules require organizations to review and modify, when necessary, their formally documented security policies and procedures on a regular basis. Due to concerns over data leakage, DHHS has provided specific guidance for addressing the emerging threat of EPHI disclosure through uncontrolled storage devices and unapproved network access that must be addressed by HIPAA regulated organizations.

SafeGuard PortProtector helps you regain control of your endpoints and address data leakage and targeted attack threats. This chapter provides guidance on how to address these threats within a HIPAA regulated environment.

The first section, *Pre-Requisites for Addressing HIPAA Data Leakage Issues*, examines organizational issues and pre-requisites that must be addressed prior to implementing SafeGuard PortProtector security features and settings. It contains the following sub-sections:

- *Foundations* translate business objectives into a HIPAA compliant context.
- *Considerations* describe the information security threats that must be addressed within the context of the established business mission.
- *Preparations* describes the activities that should be performed before configuring SafeGuard PortProtector for EPHI protection

The second section, *Implementing SafeGuard PortProtector in a HIPAA Regulated Organization*, provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product. It contains the following sub-sections:

- Implementation Approaches describes the different implementation approaches suggested in this document.
- Policy Settings describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a HIPAA environment.
- Other SafeGuard PortProtector Settings describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the HIPAA organization.
- HIPAA Security Rule / SafeGuard PortProtector Feature Mapping provides additional advice on how SafeGuard PortProtector helps to meet HIPAA Security Rule requirements.

## 13.1 Pre-Requisites for Addressing HIPAA Data Leakage Issues

SafeGuard PortProtector provides many security features that can address the threats of data leakage and targeted attacks. In order to effectively utilize the capabilities of the product, the HIPAA regulated organization should take some preliminary actions to prepare to use SafeGuard PortProtector for HIPAA compliance.

There are three categories of pre-requisites that help to ensure effective SafeGuard PortProtector implementation for HIPAA compliance. The first category is *Foundations*. Foundations are basic information security program elements that must be in place in order for any compliance effort to move forward. Foundations include the establishment of business mission statements, and roles, responsibilities required to carry them out. The second pre-requisite is *Considerations*. Considerations are specific information security threats that must be addressed within the context of the established business mission. In this case considerations are specific issues regarding the protection of EPHI in light of data leakage threats. The third pre-requisite for effective implementation is *Preparations*. Preparations are activities that must be performed prior to installing and configuring a specific technology product such as SafeGuard PortProtector.

### 13.1.1 Foundations

The implementation of new technology into an organization requires a context of business objectives. For HIPAA regulated organizations that context is provided by the following set of foundations that translate business objectives into a HIPAA compliant context for the implementation of technology.

**Foundation 1 - HIPAA Compliance Program:**

A well developed HIPAA compliance program will have implemented a business cycle of review (through risk assessment) and revision of formally documented security policies, procedures, and safeguards. Without such a program the implementation of technology is driven by a limited set of objectives focusing solely on information technology issues. For these reasons it is important to have a strong HIPAA compliance program, supporting business objectives, in place before tailoring the settings of any safeguard to comply with HIPAA requirements.

**Foundation 2 - Understand Business Needs:**

The decision to expose EPHI to data leakage threats through the use of portable mobile devices and EPHI offsite transport should be based on the neccessity of implementing business objectives. There are a variety of business objectives that may lead to the decision to allow the use of portable mobile devices and offsite transport such as home healthcare, use of PDAs in healthcare applications, or transport of medical information to offsite storage. Such a variety of business objectives leads to a variety in formally documented security policies and the application and configuration of technologic controls. These formal policies are therefore tailored to business objectives and drive the implementation of technology.

### 13.1.2 Considerations

To protect EPHI security and privacy from unauthorized access, there are a variety of security safeguards (administrative, physical, and technical) that can be used. A coordinated integration of combined safeguards is required to properly protect EPHI. The DHHS security guidance for remote use and access describes several considerations for safeguard enhancement to address this issue. Each of these “considerations” is described below as a recommended element of the HIPAA compliance program to be implemented along with the installation and configuration of SafeGuard PortProtector. Within the description of each of these considerations a set of instructions is also provided to assist in the preparation of SafeGuard PortProtector integration and configuration.

**Consideration 1 - Policies and Procedures:**

A formally documented security policy is a statement of management’s intent for protecting corporate assets from fraud, waste, and abuse. With the emergence of the data leakage threat data access policies and procedures must be reviewed and revised. The principle of least privilege, which states that each user / device should be granted only the level of access required to perform the job, needs to be interpreted to address portable media and devices.

**Instructions:**

- Ensure that your current policies are based on the principle of “Default – No Access”. This principle dictates that by default all users have no access to any corporate resources. If no such policy statement exists – create one.
- Develop guidance that interprets the “Default – No Access” policy and the “Least Privilege” policy to the roles within your organization and to the computing devices within your organization.
- Develop procedures for handling exceptions to the policies. These exceptions will be based on operational needs such as media backup, data transfer, and remote access to networks for telecommuting. Each procedure should address the risk through compensating controls such as policy, sanctions, asset tracking, multi-factor authentication, oversight, and encryption.

**Consideration 2 - Training:**

**Effective security awareness** and training is an important element of EPHI protection. HIPAA security and privacy training programs need to be periodically updated to reflect changes in threats and organizational policies. A project to update security awareness and training program should be part of the overall data leakage risk mitigation project.

**Instructions:**

- Update annual security awareness training and periodic security awareness reminders to include a discussion of data leakage threats, updated policies, user actions required, behavior prohibited, and devices restricted.
- WiFi Threats: use on unapproved networks, rogue networks, hybrid network bridging
- Mobile / Storage Device Threats: physical loss, data removal, malicious code insertion

**Consideration 3 - Incident Response.**

In the event of a security breach, resulting in the disclosure of EPHI, HIPAA regulated organizations are required to have formally documented security policies, procedures, and the capability of investigating the incident. As the set of possible security incidents expands to include data leakage, organizations must update their policies, procedures, and capabilities to respond to these incidents.

**Instructions:**

- Update incident response procedures to address data leakage issues. Specifically, create procedures for the following incident types.
- Lost or stolen mobile / storage device
- Found rogue network
- Found hybrid network bridging
- Unapproved data removal

### 13.1.3 Preparations

SafeGuard PortProtector allows organizations to control access and protect endpoints based on user roles, network domains, computer types, and criticality of systems and data. The specific implementation and configuration of SafeGuard PortProtector requires an accurate knowledge of objects SafeGuard PortProtector is to protect, the formally documented security policies it is to enforce, and the administrative roles that will maintain the SafeGuard PortProtector software. The following activities are an important element of the preparation to install and configure SafeGuard PortProtector for EPHI protection.

**Preparation 1 - Determine Endpoint Protection Needs:**

SafeGuard PortProtector protects endpoints of your network from data leakage and targeted attacks. SafeGuard PortProtector provides the ability to lock down these endpoints from data leakage through physical ports and devices and a variety of attacks and vulnerabilities. On the other hand your organization has a variety of business needs that will require connectivity to external storage devices, wireless networks, and other possible threats. In preparation for a SafeGuard PortProtector deployment your organization should determine the protection and business needs of the endpoints.

**Instructions:**

- Update endpoint inventory and classification. Be sure that you are aware of all your endpoints within your network that store, process, or transmit EPHI. This can be done through a manual inventory process or through the use of directory services. Classification is based on your data classification policy and includes a classification of endpoints that handle EPHI data.
- Scan each endpoint to detect port, device, and WiFi usage. The SafeGuard PortAuditor will automatically detect devices and networks that are currently or previously connected.
- Review your “Default – No Access” and “Least Privilege” policies as they apply to the endpoints that have now been inventoried, classified, and scanned. Make a list of the intended profiles for each endpoint classification.

**Preparation 2 - Determine User Access Roles**

SafeGuard PortProtector allows for the specification of allowed ports, devices, and WiFi usage according to user, user group, or organizational unit as defined by Active Directory or Novel eDirectory. It is important to note that any user privileges granted through this mechanism will trump those specified for an individual endpoint. For example, if you set up a user to have WiFi access and have also locked down a laptop to block WiFi access through SafeGuard PortProtector, that user will be able to gain WiFi access through that laptop based on his SafeGuard PortProtector user profile. With this rule in mind it is strongly recommended that you be very careful when creating any user privileges. User privileges will supersede any restrictions placed on endpoints.

**Instructions:**

Determine user roles within your SafeGuard PortProtector implementation.

- User – this role is the normal user role that has no additional privileges other than the privileges that are common throughout the organization.
- Privileged user – this role has extended privileges (for example - the ability to write files to a USB device or connect to a WiFi network).

Determine compensating controls placed on privileged users.

- Logs and alerts – at a minimum plan to set privileged user policies to log allowed behavior that is extended from the normal user role. Consider setting alerts on highly sensitive behavior such as connecting an external hard disk.

**Preparation 3 - Determine Administration Roles**

SafeGuard PortProtector allows for multiple administration roles according to roles and organizational structure. The use of these administrative role options should be determined prior to installation of SafeGuard PortProtector.

**Instructions:**

- Determine if your implementation of SafeGuard PortProtector will follow a centralized or de-centralized administration model.
- Centralized – a single entity is responsible for the administration of SafeGuard PortProtector.
- De-centralized – administration of SafeGuard PortProtector is delegated to departments that are responsible for the administration of their own part of the domain. If you chose this method of administration, then determine the domain partitions for which each department will be responsible for the administration.
- Determine administration roles within each domain.

- The SafeGuard PortProtector administrator may be set up as a single role or you may delegate administrative privileges to implement separation of duties. Determine the set of administrative roles that you will implement.
- Plan maintenance and incident response function for SafeGuard PortProtector administration.
- Incident response – those responsible for responding to incidents involving lost or stolen storage devices, rogue networks, hybrid network bridging, or unapproved data removal will require special permissions within SafeGuard PortProtector and access to audit tools. Document the incident response roles within your organization and the permissions and access required.
- Maintenance – those responsible for handling end user issues such as peripherals and network connectivity will require the ability to request modifications to object or user permissions. Document maintenance roles within your organization and the permissions and access required.

## 13.2 Implementing SafeGuard PortProtector in a HIPAA Regulated Organization

This section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product.

- Implementation Approaches describes the various implementation approaches suggested in this document.
- Policy Settings describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a HIPAA environment.
- Other SafeGuard PortProtector Settings describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the HIPAA organization.
- HIPAA Security Rule / SafeGuard PortProtector Feature Mapping provides additional advice on how SafeGuard PortProtector helps to meet HIPAA Security Rule requirements.

### 13.2.1 Implementation Approaches

The HIPAA Security Rule requires HIPAA regulated organizations to protect EPHI through a set of required and addressable standards (The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334). However, the HIPAA Security Rule does not specify precisely how to implement these safeguards or what mechanisms must be employed. Since each organization has its own unique business objectives, there will be a variety of HIPAA implementations throughout the HIPAA regulated organization community. In an effort to address these differing implementations this document provides guidance for both a “Standard” and an “Aggressive” approach for implementing SafeGuard PortProtector to protect EPHI. Both of these approaches meet the HIPAA standards for the requirements they address.

**Standard Approach:** The standard approach to implementing SafeGuard PortProtector within a HIPAA environment implements good security practices for protecting endpoints from targeted attacks and ensuring that potential data leakage of EPHI is monitored and logged.

**Aggressive Approach:** The aggressive approach to implementing S SafeGuard PortProtector within a HIPAA environment implements a more strict set of security practices for protecting endpoints from targeted attacks and ensuring that potential data leakage of EPHI is blocked, encrypted, or monitored and logged.

The selection of the appropriate approach for meeting both HIPAA and an organization's business objectives maybe either the Standard Approach, the Aggressive Approach, or even a combination or customization of either of these approaches. Recall "Foundation 2: Understand Business Needs" (*see above*) from part 1 of this whitepaper, which stresses the importance of understanding the business objectives and environment in which SafeGuard PortProtector is to be deployed prior to determining the configuration and setting of the product. Just as technology implementation to meet HIPAA requirements is flexible, so is the configuration of SafeGuard PortProtector. The flexibility is designed to meet the variety of business objectives of HIPAA regulated organizations.

## 13.2.2 Policy Settings

The following table is a guide to the SafeGuard PortProtector administrator in the setting and configuration of SafeGuard PortProtector for implementation within a HIPAA environment. The standard and aggressive approaches are to be used as guidelines for setting the parameters of SafeGuard PortProtector and not to be interpreted as additional HIPAA requirements. In fact the HIPAA security rule does not specify protection requirements down to this level of detail. However, these configuration settings do follow general security principles and can be used as a baseline in creating a policy set for your own organization.

| Setting | Standard HIPAA Approach | Aggressive HIPAA Approach | Rationale |
|---|---|---|---|
| **Policy** | | Create new policies based on the built-in policy of Standard HIPAA or Aggressive HIPAA. Each policy can then be modified as determined by the HIPAA compliance officer and in accordance with the organization's business objectives. | |
| **Port Control:** | | | |
| **USB** | Restrict | Restrict | Restricting access to these ports allows for a finer granularity of control under the device control section of the policy-security. |
| **FireWIre** | Restrict | Restrict | |
| **PCMCIA** | Restrict | Restrict | |
| **SD** | Allow | Allow | Allowing access to these ports is required for some standard human interface devices. The access restrictions to these ports for storage devices will be further restricted through storage control below. |
| **Serial** | Allow | Allow | |
| **Parallel** | Allow | Allow | |
| **WiFi** | Restrict | Restrict | Restricting access to WiFi networks allows for a finer granularity of control under the WiFi |

| Setting | Standard HIPAA Approach | Aggressive HIPAA Approach | Rationale |
|---|---|---|---|
| | | | control section of the policy-security. |
| **Modem** | Allow + log | Allow + log | Use of Modem, IrDA, or Bluetooth can lead to unauthorized network connections. At a minimum use of these ports should be logged.<br>A more aggressive posture would block and log IrDA and Bluetooth links. |
| **IrDA** | Allow + log | Block + log | |
| **Bluetooth** | Allow + log | Block + log | |
| **Network Bridging** | Block (All) | Block (All) | Blocking user access to WiFi, Bluetooth, Modems, and IrDA links while connected to the TCP/IP network interface protects endpoints from the dangerous practice of hybrid network bridging. |
| Device Control | | | |
| **Hardware Keyloggers** | Allow | Allow | Although the use of hardware keyloggers should be restricted and users should be protected from these attacks, usability concerns override the need for this restriction. |
| **Human Interface** | Allow | Allow | It is typically not considered a risky practice to allow users to connect to human interface devices such as keyboards and mice. |
| **Printers** | Allow | Allow | Although a printer can be a data leakage source, printing is a common user function within most organizations. Compared to storage devices and PDAs, printers have a much lower capacity to “leak” large amounts of EPHI. This risk can be mitigated by physical |

| Setting | Standard HIPAA Approach | Aggressive HIPAA Approach | Rationale |
|---|---|---|---|
| | | | and administrative controls. |
| PDA<br>Mobile Phones<br>Imaging<br>Audio / video Devices | Allow + Log | Restrict, White List, Log | PDAs, mobile phones, Imaging devices (such as scanners) and Audio / Video devices (such as MP3 players) present a clear risk to the control and protection of EPHI. At a minimum a HIPAA organization should log any such behavior. A more aggressive setting to not only log the behavior but restrict use to an approved list of devices such as company issued PDAs. |
| Network Adapters | Allow | Allow | Network adapters allow the PC to be connected to a network. This is a common configuration and should not be blocked or logged. |
| Smart Cards | Allow | Allow | Smart Cards are common as an authentication device. They do not pose a reasonable threat to EPHI data. |
| Content security devices | Allow | Allow | Content security devices monitor the content of the flow of data to and from the endpoint. If such devices are present they are part of a solution to enforce security and should not be blocked at the endpoint. |
| Unclassified devices | Block + Log | Block + Log | Unclassified devices are any devices that are not otherwise specified. These should not turn up very often, and present a risk to EPHI control and protection. |
| Storage Control | | | |

| Setting | Standard HIPAA Approach | Aggressive HIPAA Approach | Rationale |
|---|---|---|---|
| **Autorun function** | Block | Block | A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default. |
| **Removable storage** | Allow + log<br>Block smart function | Encrypt + log<br>Block smart function | Storage devices (such as USB drives) present a clear risk to EPHI control and protection. At a minimum a HIPAA organization should log use of storage devices. A more aggressive approach would restrict the use of storage devices to approved devices.<br>A more aggressive approach would also ensure that EPHI written to storage devices is encrypted; providing further protection in the event the storage device is lost or stolen.<br>Certain formats for writing files to media such as CD or DVD do not support the event logging. In the aggressive HIPAA setting to preserve the logging settings for all files this option should remain checked. |
| **External HD** | Allow + log | Encrypt + log | |
| **CD/DVD** | Allow + log<br>Allow unsupported formats | Encrypt + log<br>Block unsupported formats | |
| **Floppy Drives** | Allow + log | Read only + log | |
| **Tape Drives** | Allow + log | Restrict + log | |
| **File Control** | Allow + Log (write only) | Allow + Log (write only) | In order to support audit and investigation of security incidents involving EPHI log all files written to external storage devices. |
| **WiFi** | Allow + Log | Restrict networks, block | Wireless networks |

| Setting | Standard HIPAA Approach | Aggressive HIPAA Approach | Rationale |
|---|---|---|---|
| **Network** | | peer to peer, White List | present a clear risk to the control and protection of EPHI. At a minimum a HIPAA organization should log any such behavior. A more aggressive setting to not only log the behavior but restrict use to an approved list of WiFi networks that have been approved by the organization and have proper encryption. |
| **Policy Settings** | | | |
| **Logging** | Send logs to SafeGuard PortProtector Server<br>Send logs every 12 hours or less.<br>Log connect and disconnect events | Send logs to SafeGuard PortProtector Server<br>Send logs every 12 hours or less.<br>Log connect and disconnect events | Logs should clearly not be stored on the endpoint, but instead sent to the SafeGuard PortProtector Server where they can be protected and viewed by the administrator.<br>Other logging settings here provide adequate EPHI protection by ensuring periodic updating of logs on the server without burdening the network; inclusion of connect and disconnect events to allow for analysis of how long a device was connected; |
| **End-user messages** | Review the end user messages associated with the HIPAA setting to ensure they are consistent with your formally documented security policies and security awareness training program. | | It is important to provide a constant reminder to those exposed to EPHI that they are responsible for protecting EPHI and complying with policies. Modifying the end-user messages to specifically mention HIPAA security and EPHI protection will assist in the security awareness of your organization. |

| Setting | Standard HIPAA Approach | Aggressive HIPAA Approach | Rationale |
|---|---|---|---|
| **Encryption** | None | Do not allow users to access encrypted devices at home<br><br>Approve read only access for non-encrypted devices. | It is important to restrict the use of EPHI to systems with adequate protection measures. Home computers generally lack HIPAA required security controls.<br><br>Setting read-only for non-encrypted devices allows the flexibility of importing information without exposing EPHI to the risk of disclosure from loss or theft of a non-encrypted device. |
| **Options** | Use a different password from the client administration password to uninstall SafeGuard PortProtector<br><br>Full visibility on endpoints | Use a different password to uninstall SafeGuard PortProtector<br><br>Full visibility on endpoints | In order to enforce the principle of separation of duty and general password security, use a different password for the uninstall process of SafeGuard PortProtector Client than the client administration password.<br><br>Consistent with the advice under “end user messages” it is best to let users know about the protections SafeGuard PortProtector is providing to EPHI. |

## 13.2.3 Other SafeGuard PortProtector Settings

For the appropriate setting of other SafeGuard PortProtector features and options refer to *Pre-Requisites for Addressing HIPAA Data Leakage Issues* detailed in part 1 of the HIPAA Security Compliance with SafeGuard PortProtector document. Specifically, the following SafeGuard PortProtector features should follow the business objectives and the environment of the HIPAA organization as defined in foundations, considerations, and preparations.

**Alerts**

SafeGuard PortProtector alerts provide oversight of administrative actions and protection of the SafeGuard PortProtector security functions in case of attempted tampering. The following alert options should be set in order to preserve the security functions provided by SafeGuard PortProtector:

Log all administrative events: Logs all administrative actions and provides oversight of SafeGuard PortProtector administration.

Alert all tempering events: Detects tempering attempts and ensures the integrity of end point protection controls.

**SafeGuard PortProtector Administration**

SafeGuard PortProtector may be run by a single administrator or an organization may implement additional access control by defining additional administrators to a subset of administrative functions. This is an implementation of role-based access control and should be considered based on the organizations approach as defined in "Preparation 3: Determine Administrative Roles." Among the roles a HIPAA organization should consider are the following:

- Log Reviewer: Access to all logs and log functions without ability to edit policies.
- Policy Administrator: Access to edit and administer policies without ability to view logs.
- Audit: Read-only access to administrators console without ability to perform any changes.

The setting of these roles should be based on the administration model and approach of the organization and the support needed for incident response and maintenance. Refer to Part 1 of this whitepaper for more complete instructions for SafeGuard PortProtector implementation *Preparations*.

**Domain Partitioning**

Further access control granularity may be added with the SafeGuard PortProtector domain partitioning feature. The role based access mechanism includes domain partitioning, which allows an administrator role to be limited to a specific group of clients. This feature is useful in restricting the administrator's access to sensitive domains such as those domains which contain EPHI. The setting of these roles should be based on the organization's administration model and approach and the support needed for incident response and maintenance. Refer to Part 1 of this whitepaper for more complete instructions for the SafeGuard PortProtector implementation preparation.

**Administrative Password Strength**

All passwords that protect EPHI within a HIPAA organization must comply with the organization's formally documented password policies. Formally documented security policies are discussed in more detail in "Consideration 1: Policies and Procedures" in part 1 of this document. Based on the organization's password strength policy, SafeGuard PortProtector administrative password strength criteria should be defined in the SafeGuard PortProtector to enforce organizational policies. Elements of the password strength include minimum length and required character types.

## 13.2.4 HIPAA Security Rule / SafeGuard PortProtector Feature Mapping

SafeGuard PortProtector provides HIPAA organizations additional technical controls to protect EPHI at system endpoints and address data leakage and target attack threats. As discussed throughout this paper SafeGuard PortProtector can address data leakage risks, targeted attack threats, and many of the HIPAA Security Rule requirements. Although obvious, it should be noted that SafeGuard PortProtector provides a portion of the technical controls (and influences some administrative controls) necessary for complete HIPAA compliance. The table below provides additional advice on how SafeGuard PortProtector helps to meet HIPAA Security Rule requirements.

| **HIPAA** | | | |
|---|---|---|---|
| Section of HIPAA Security Rule | Rule Description | Relevant SafeGuard PortProtector Features | How to Satisfy HIPAA Controls with SafeGuard PortProtector |
| **Physical Safeguards** | | | |
| 164.310(d)(1) | Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | SafeGuard PortProtector provides the ability to control access to portable storage devices such as USB drives, PDAs, and mobile phones. The flexibility of SafeGuard PortProtector policies allow for a granularity of control that matches a HIPAA organization's needs. Options include the ability to record connection and disconnection of devices and media. | Configure SafeGuard PortProtector to control media and storage device use on the organization's desktops and laptops. Two built-in HIPAA approaches provide reasonable approaches and rationale for these settings.<br>Review logs according to organization policy and procedures. |

| IPAA | | | |
|---|---|---|---|
| Section of HIPAA Security Rule | Rule Description | Relevant SafeGuard PortProtector Features | How to Satisfy HIPAA Controls with SafeGuard PortProtector |
| **Administrative Controls** | | | |
| 164.308(a)(1)(i) | Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations. | SafeGuard PortProtector is a technology control that can implement policies and procedures to prevent and detect security violations at the network endpoints. | See consideration 1 [Policies and Procedures] for instructions on what policies and procedures need to be implemented.<br>SafeGuard PortProtector has built-in security policies for "Standard HIPAA Approach" and "Aggressive HIPAA Approach". Associate built-in policies for either HIPAA approach with your users and machines that may have EPHI access. If your organization chooses to deviate from built-in HIPAA policies, document business reason and compensating controls. |

| | | | |
|---|---|---|---|
| 164.308(a)(1)(ii)(A) | Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the organization. | SafeGuard PortAuditor provides a full view of the ports, devices and networks in use by your organization's users, as well as a history of what was used previously. The SafeGuard PortAuditor scan output can select the devices and networks to control. Left uncontrolled, all of these devices provide vulnerability for the misuse of EPHI. | Utilize SafeGuard PortAuditor during the data gathering phase. Specifically, scan all endpoints for current settings (ports, peripherals, etc.) and port and device usage history. Review scan results against the current policies covering endpoint security.<br>The data leakage threat can be measured during a risk assessment by temporarily applying a policy of “allow + log”. The results could be reviewed to determine the current extent of data transfer to storage devices. |
| 164.308(a)(1)(ii)(D) | Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | SafeGuard PortProtector products collect several logs types:<br>Client Log – Information about Clients and users in the organization. Each record reports a specific event, such as the connection of a detachable device to a computer, or a tampering attempt.<br>File Log – File information for removable storage devices, external hard disks or CD/DVD<br>Server Log – Information about the Management Server and administrative actions. Each record reports a specific event, such as logging into the Management Console, and changing Global Policy Settings. | Configure SafeGuard PortProtector to collect logs and send alerts according to your organizations policy. Two built-in HIPAA approaches provide reasonable approaches and rationale for these settings.<br>Review logs according to organization policy and procedures. |

| **HIPAA** | | | |
|---|---|---|---|
| Section of HIPAA Security Rule | Section of HIPAA Security Rule | Section of HIPAA Security Rule | Section of HIPAA Security Rule |
| **Technical Safeguards** | | | |
| 164.312(a)(2)(iv) | Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. | Using the policy manager, user behavior is controlled at the endpoint. Depending on the connected device, SafeGuard PortProtector can force all information directed to a specific device to be encrypted.<br>As a rule, organizationally-encrypted removable storage devices can be used only when connected to protected endpoints. An optional function allows or prohibits content from being opened on non-organizational computers.<br>For Non-encrypted Devices, policies can be deployed that determine behavior when a non-encrypted device is detected; the device may either be blocked, or permitted Read Only access.<br>Wireless networks can be controlled at the endpoint. Two types of control are available:<br>Specify which connection types are allowed access<br>Determine which specific networks are allowed access. | SafeGuard PortProtector extends the ability to enforce encryption policies and procedures within a HIPAA organization. SafeGuard PortProtector can enforce these procedures by blocking attempts to read or write unencrypted devices, and guide the user in the process of encrypting an unencrypted device.<br>blocking the use of encrypted devices outside the organization ensuring wireless communication is restricted to properly encrypted and approved wireless networks. |

| | | | |
|---|---|---|---|
| 164.312(b) | Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI | SafeGuard PortProtector records endpoint events associated with storage devices and media in client logs. An event may be a device connection or disconnection, a wireless network connection, tampering attempts or administrator login. Event logs include endpoint identify, user, event type, and time.<br>SafeGuard PortProtector also creates server logs for administrative events such as administrator login, publishing policies and performing backups.<br>Client and Server logs are sent to a log repository and stored on the Management Server at the defined intervals. | Configure SafeGuard PortProtector to collect client and server logs according to your organizations policy. Built-in management, operational, and audit reports collect and organize critical data that allows for the efficient examination of activities related to data transfer to storage devices and media. |
| 164.312(e)(2)(ii) | Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | Policies can be created that either force data to be encrypted before being transferred to removable storage devices, or force the use of encrypted WiFi channels for secure transfer of data. | SafeGuard PortProtector extends the ability to enforce encryption policies and procedures within a HIPAA organization.<br>blocking attempts to write to unencrypted devices<br>blocking the non-network use of encrypted devices<br>ensuring wireless communication is restricted to properly encrypted and approved wireless networks. |

# 14 Appendix F – Using SafeGuard PortProtector in a SOX Regulated Organization

## About This Appendix

In response to the major corporate accounting scandals at the beginning of the millennium, the United States enacted a public law entitled "Public Company Accounting Reform and Investor Protection Act of 2002." This law is generally referred to by its shorter nickname in honor of the major sponsors of the act, Senator Paul Sarbanes (D-MD) and Representative Michael Oxley (R-OH), thus Sarbanes-Oxley or SOX. The law contains many titles and provisions but the area of most concern regarding information security is section 404: Assessment of internal control.

SOX section 404 requires, among other things, for an external auditor to evaluate the controls for safeguarding assets. This review of controls by an external auditor is typically guided by the Common Objectives of Information and Related Technology (COBIT) as an internal control framework. Recent data losses and attacks at the endpoint have highlighted the need for protection at all levels of the network, including network endpoints. Ensuring security at the endpoints within a network is one of the issues that must be addressed by all organizations seeking to meet SOX requirements.

SafeGuard PortProtector helps you regain control of your endpoints and address data leakage and targeted attack threats. This chapter provides guidance on how to address these threats within a SOX 404 regulated environment.

The first section *Pre-Requisites for Addressing SOX Compliance Issues*, examines organizational issues and pre-requisites that must be addressed prior to implementing SafeGuard PortProtector security features and settings. It contains the following sub-sections:

- Foundations translates business objectives into a SOX compliant context.
- Considerations describes the information security threats that must be addressed within the context of the established business mission.
- Preparations describes the activities that should be performed before configuring SafeGuard PortProtector for protection.

The second section, *Implementing SafeGuard PortProtector in a SOX Regulated* Organization, provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product. It contains the following sub-sections:

- Implementation Approaches describes the different implementation approaches suggested in this document.
- SOX policy settings describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a SOX environment.
- Other SafeGuard PortProtector SOX Settings describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the SOX organization.
- Relevant SOX Requirements provides additional information on SOX Security Rule requirements.

## 14.1 Pre-Requisites for Addressing SOX Compliance Issues

SafeGuard PortProtector provides many security features that can address the threats of endpoint security. In order to effectively utilize the capabilities of the product, the SOX regulated organization should take some preliminary actions to must prepare to use SafeGuard PortProtector for SOX 404 compliance.

There are three categories of pre-requisites for effective implementation of SafeGuard PortProtector for SOX 404 compliance. The first category is *Foundations*. Foundations are basic information security program elements that must be in place in order for any compliance effort to move forward. Foundations include the establishment of business mission statements, and roles, responsibilities required to carry them out. The second pre-requisite is *Considerations*. Considerations are specific information security threats that must be addressed within the context of the established business mission. The third pre-requisite for effective implementation is *Preparations.* Preparations are activities that must be performed prior to installing and configuring a specific technology product such as SafeGuard PortProtector.

### 14.1.1 Foundations

The evaluation of security controls within an organization requires a context of business objectives. For SOX regulated organizations that context is provided by the following set of foundations that translate business objectives into a SOX 404 compliant context for the implementation of technology.

**Foundation 1: Information Security Program**

An information security program consists of dedicated security professionals supported by management with the appropriate scope, authority, and budget to assess information security risks, recommend mitigation techniques and ensure appropriate security risk management of the organization’s assets. A strong information security program will include an identification of reasonable threats to the organization’s assets, a review of the physical, administrative, and technical controls, and the planning and implementation oversight of security controls to bring the security posture to an acceptable assurance level.

**Foundation 2: Audit Program**

An organization seeking to comply with SOX must have an existing internal audit program. Such a program comprises the policies and procedures that govern the internal audit function. At a minimum an internal audit program includes an audit charter (establishing the audit function), annual risk assessments, an audit plan (goals, schedules, and staffing for audit), and audit processes for the audit cycle, audit efforts, audit reports, and audit documentation.

### 14.1.2 Considerations

To ensure the protection of the organization’s assets there are a number of control objectives that must be met. Prior to embarking on an effort to implement these control objectives SOX organization should first consider several key elements of the upcoming SOX 404 compliance project. Careful consideration of these elements can help an organization avoid several common pitfalls and increase its efficiency in the SOX 404 compliance effort.

**Consideration 1: Control Objectives**

Common Objectives of Information and Related Technology (COBIT) is an internal control framework used as a guide by external auditors to review the effectiveness of the controls on your internal financial systems. It is important to remember that COBIT is a guide and can be tailored to meet your business objectives by choosing appropriate control objectives and compensating controls where applicable. Work with your external audit team to develop the appropriate set of control objectives for your organization. As the COBIT and the audit process can seem foreign to many within the IT department, the addition of a Certified Information System Auditor (CISA) to your internal team overseeing the external audit can create efficiencies in your SOX 404 compliance project.

**Instructions:**

- Work with external audit team to develop an appropriate set of control objectives.
- Review reasonableness and completeness of proposed control objectives.
- Add a Certified Information System Auditor (CISA) to your internal team working with the external auditors.

**Consideration 2: Policies and Procedures**

A security policy is a statement of management's intent for protecting corporate assets from fraud, waste, and abuse. With the emergence of the data leakage threat data access policies and procedures must be reviewed and revised. The principle of least privilege, which states that each user should be only the level of access required to perform their job, needs to be interpreted to address portable media and devices.

**Instructions:**

- Ensure that your current policies are based on the principle of "Default – No Access". This principle dictates that by default all users have no access to any corporate resources. If no such policy statement exists – create one.
- Develop guidance that interprets the "Default – No Access" policy to the roles within your organization and to the computing devices within your organization.
- Develop procedures for handling exceptions to the "Default – No Access" policy. These exceptions will be based on operational needs such as media backup, data transfer, and remote access to networks for telecommuting. Each procedure should address the risk through compensating controls such as policy, sanctions, asset tracking, multi-factor authentication, oversight, and encryption.

**Consideration 3: Training**

Effective security awareness and training is an important element of asset protection. Information security training programs need to be periodically updated to reflect changes in threats and organizational policies. A project to update security awareness and training program should be part of the overall data leakage risk mitigation project.

**Instructions:**

- Update annual security awareness training and periodic security awareness reminders to include a discussion of data leakage threats, updated policies, user actions required, behavior prohibited, and devices restricted.
- Wi-Fi Threats: use on unapproved networks, rogue networks, hybrid network bridging, WEP authentication.
- Mobile / Storage Device Threats: physical loss, data removal, malicious code insertion

**Consideration 4: Incident Response**

In the event of a security breach resulting in the disclosure, modification, or interruption of service, SOX 404 compliant organizations are required to have policies, procedures, and the capability of investigating the incident. As the set of possible security incidents expands to include data leakage, organizations must update their policies, procedures, and capabilities to respond to these incidents.

**Instructions:**

- Update incident response procedures to address data leakage issues. Specifically, create procedures for the following incident types.
- Lost or stolen mobile / storage device
- Found rogue network
- Found hybrid network bridging
- Unapproved data removal

### 14.1.3 Preparations

SafeGuard PortProtector allows organizations to control access and protect endpoints based on user roles, network domains, computer types, and criticality of systems and data. The specific implementation and configuration of SafeGuard PortProtector requires an accurate knowledge of objects SafeGuard PortProtector is to protect, the policies it is to enforce, and the administrative roles that will maintain the SafeGuard PortProtector software. The following activities are an important element of the preparation to install and configure SafeGuard PortProtector the implementation of appropriate internal controls.

**Preparation 1: Determine Endpoint Protection Needs**

SafeGuard PortProtector provides the ability to protect stored data for uncontrolled export on removable devices at endpoints. On the other hand your organization has a variety of business needs that will require connectivity to external storage devices, wireless networks, and other possible threats. In preparation for a SafeGuard PortProtector deployment your organization should determine the protection and business needs of the endpoints.

**Instructions:**

- Update endpoint inventory and classification. Be sure that you are aware of all the endpoints within your network that store, process, or transmit sensitive data. This can be done through a manual inventory process of through the use of directory services. Classification is based on your data classification policy and includes a classification of endpoints that handle sensitive data.
- Scan each endpoint to detect port, device, and Wi-Fi usage. The SafeGuard PortAuditor utility will automatically detect devices and networks that are currently or previously connected.
- Review your “Default – No Access” and least privilege policies as they apply to the endpoints that have now been inventoried, classified, and scanned. Make a list of the intended profiles for each endpoint classification.

**Preparation 2: Determine User Access Roles**

SafeGuard PortProtector allows for the specification of allowed ports, devices, and Wi-Fi usage according to user, user group, or organizational unit as defined by Active Directory or Novel eDirectory. It is important to note that any user privileges granted through this mechanism will trump those specified for an individual endpoint. For example, if you set up a user to have Wi-Fi access (over WPA networks) and have also locked down a laptop to block Wi-Fi access, that user will be able to gain Wi-Fi access through that laptop. With this rule in mind it is strongly recommended that you be very careful when creating any user privileges as those privileges will apply to any endpoint to into which that user logs.

**Instructions:**

- Determine user roles within your SafeGuard PortProtector implementation.
- User – this role is the normal user role that has no additional privileges associated.
- Privileged user – this role has extended privileges such as the ability to write files to a USB device or connect to a WPA-enabled Wi-Fi network.
- Determine compensating controls placed on privileged users.
- Logs and alerts – at a minimum plan to set privilege user policies to log allowed behavior that is extended from the normal user role. Consider setting alerts on highly sensitive behavior such as connecting and external hard drive.

**Preparation 3: Determine Administration Roles**

SafeGuard PortProtector allows for multiple administration roles according to privilege and domain. The use of these administrative role options should be determined prior to installation of SafeGuard PortProtector.

**Instructions:**

- Determine if your implementation of SafeGuard PortProtector will follow a centralized or de-centralized administration model.
- Centralized – a single entity is responsible for the administration of SafeGuard PortProtector.
- De-centralized – administration of SafeGuard PortProtector is delegated to departments that are responsible for the administration of their own domain. If you chose this method of administration, then determine the domain partitions for which each department will be responsible for the administration.
- Determine administration roles within each domain.
- The SafeGuard PortProtector administrator may be set up as a single role or you may delegate administrative privileges to implement separation of duties. Determine the set of administrative roles that you will implement.
- Plan maintenance and incident response function for SafeGuard PortProtector administration.
- Incident response – those responsible for responding to incidents involving lost or stolen storage devices, rogue networks, hybrid network bridging, or unapproved data removal will require special permissions within SafeGuard PortProtector and access to audit tools. Document the incident response roles within your organization and the permissions and access required.
- Maintenance – those responsible for handling end user issues such as peripherals and network connectivity will require the ability to request modifications to object or user permissions. Document maintenance roles within your organization and the permissions and access required.

## 14.2 Implementing SafeGuard PortProtector in a SOX Regulated Organization

This section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product.

- Implementation Approaches describes the different implementation approaches suggested in this document.
- SOX policy settings describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a SOX regulated environment.
- Other SafeGuard PortProtector SOX Settings describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy.
- Relevant SOX Requirements provides additional information on the SOX Security Rule requirements.

## 14.2.1 Implementation Approaches

The SOX 404 / COBIT regulation requires SOX regulated organizations to provide adequate internal controls. However, the SOX 404 / COBIT does not specify precisely how to implement these safeguards or what mechanisms must be employed. Since each organization has its own unique business objectives, there will be a variety of COBIT implementations throughout the SOX regulated organization community]. In an effort to address these differing implementations this document provides guidance for both a “Standard” and an “Aggressive” approach for implementing SafeGuard PortProtector to protect the organization’s assets. Both of these approaches meet the SOX 404 / COBIT standards for the requirements they address.

**Standard Approach:** The standard approach to implementing SafeGuard PortProtector within a SOX regulated environment implements good security practices for protecting endpoints from targeted attacks and ensuring that adequate internal controls for the protection of data leakage at network endpoints.

**Aggressive Approach:** The aggressive approach to implementing SafeGuard PortProtector within a SOX regulated environment implements a more strict set of security practices for protecting endpoints from targeted attacks and ensuring adequate internal controls for the protection of data leakage at network end points.

The selection of the appropriate approach for meeting both SOX 404 / COBIT and an organization’s business objectives maybe either the Standard Approach, the Aggressive Approach, or even a combination or customization of either of these approaches. Recall “Consideration 1: Control Objectives” under *Considerations*, which stresses the importance of understanding the business objectives and environment in which SafeGuard PortProtector is to be deployed prior to determining the configuration and setting of the product. Just as technology implementation to meet SOX 404 / COBIT requirements is flexible, so is the configuration of SafeGuard PortProtector. The flexibility is designed to meet the variety of business objectives of SOX regulated organizations.

## 14.2.2 SOX policy settings

The following table is a guide to the SafeGuard PortProtector administrator in the setting and configuration of SafeGuard PortProtector for implementation within a SOX regulated environment. The standard and aggressive approaches are to be used as guidelines for setting the parameters of SafeGuard PortProtector and not to be interpreted as additional SOX requirements. In fact the SOX regulation does not specify protection requirements down to this level of detail. However, these configuration settings do follow general security principles and can be used as a baseline in creating a policy set for your own organization.

| Setting | Standard SOX Approach | Aggressive SOX Approach | Rationale |
|---|---|---|---|
| **Policy** | | Create new policies based on the built-in policy of Standard SOX or Aggressive SOX. Each policy can then be modified as determined by the SOXcompliance officer and in accordance with the organization’s business objectives. | |
| **Port Control:** | | | |
| **USB** | Restrict | Restrict | Restricting access to these ports allows for a finer |
| **FireWIre** | Restrict | Restrict | |

| Setting | Standard SOX Approach | Aggressive SOX Approach | Rationale |
|---|---|---|---|
| **PCMCIA** | Restrict | Restrict | granularity of control under the device control section of the policy-security. |
| **SD** | Allow | Allow | Allowing access to these ports is required for some standard human interface devices. The access restrictions to these ports for storage devices will be further restricted through storage control below. |
| **Serial** | Allow | Allow | |
| **Parallel** | Allow | Allow | |
| **WiFi** | Restrict | Restrict | Restricting access to WiFi networks allows for a finer granularity of control under the WiFi control section of the policy-security. |
| **Modem** | Allow + log | Allow + log | Use of Modem, IrDA, or Bluetooth can lead to unauthorized network connections. At a minimum use of these ports should be logged.<br>A more aggressive posture would block and log IrDA and Bluetooth links.<br>Blocking user access to these links while connected to the TCP/IP network interface protects endpoints from the dangerous practice of hybrid network bridging. |
| **IrDA** | Allow + log | Block + log | |
| **Bluetooth** | Allow + log | Block + log | |
| **Network Bridging** | Block (All) | Block (All) | Blocking user access to WiFi, Bluetooth, Modems, and IrDA links while connected to the TCP/IP network interface protects endpoints from the dangerous practice of hybrid network bridging. |
| **Device Control** | | | |
| **Hardware Keyloggers** | Allow | Allow | Although the use of hardware keyloggers should be restricted and users should be protected from these attacks, usability concerns override the need for this restriction. |

| Setting | Standard SOX Approach | Aggressive SOX Approach | Rationale |
|---|---|---|---|
| **Human Interface** | Allow | Allow | It is typically not considered a risky practice to allow users to connect to human interface devices such as keyboards and mice. |
| **Printers** | Allow | Allow | Although a printer can be a data leakage source, printing is a common user function within most organizations. Compared to storage devices and PDAs, printers have a much lower capacity to “leak” large amounts of EPHI. This risk can be mitigated by physical and administrative controls. |
| **PDA**<br>**Mobile Phones**<br>**Imaging**<br>**Audio / video Devices** | Restrict, White List, Log | Restrict, White List, Log | PDAs, mobile phones, Imaging devices (such as scanners) and Audio / Video devices (such as MP3 players) present a clear risk to the control and protection of data and networks. Organizations must ensure that any use of PDAs or Mobile phones supports encryption of sensitive information. Access to such devices should be restricted to an approved list of devices such as company issued PDAs and such access should be logged. |
| **Network Adapters** | Allow | Allow | Network adapters allow the PC to be connected to a network. This is a common configuration and should not be blocked or logged. |
| **Smart Cards** | Allow | Allow | Smart Cards are common as an authentication device. They do not pose a reasonable threat to the organization's assets. |

| Setting | Standard SOX Approach | Aggressive SOX Approach | Rationale |
|---|---|---|---|
| **Content security devices** | Allow | Allow | Content security devices monitor the content of the flow of data to and from the endpoint. If such devices are present they are part of a solution to enforce security and should not be blocked at the endpoint. |
| **Unclassified devices** | Block + Log | Block + Log | Unclassified devices are any devices that are not otherwise specified. These should not turn up very often. At a minimum there connection should be logged. An aggressive setting would block access to these devices. |
| **Storage Control** | | | |
| **Autorun function** | Block autorun function | Block autorun function | A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default. |
| **Removable storage** | Encrypt + log<br>Block smart function | Encrypt + log<br>Block smart function | Storage devices present a clear risk to the organization's assets. At a minimum a SOX organization restrict the use of storage devices to approved devices.<br>Any data being written to storage devices should be encrypted; providing further protection in the event the storage device is lost or stolen. |
| **External HD** | Encrypt + log | Encrypt + log | |
| **CD/DVD** | Encrypt + log<br>Block unsupported formats | Encrypt + log<br>Block unsupported formats | |
| **Floppy Drives** | Read only + log | Read only + log | |
| **Tape Drives** | Restrict + log | Restrict + log | |

| Setting | Standard SOX Approach | Aggressive SOX Approach | Rationale |
|---|---|---|---|
| **File Control** | Allow + Log – write only | Allow + Log – write only | In order to support audit and investigation of security incidents involving EPHI log all files written to external storage devices. |
| **WiFi Network** | Allow + Log | Restrict , white list WPA encrypted networks, log | Wireless networks present a clear risk to the control and protection of data. At a minimum a SOX regulated organization should log any such behavior. However, the organization should use other internal controls to ensure that all wireless networks are secured through adequate encryption. A more aggressive setting to not only log the behavior but restrict use to an approved list of Wi-Fi networks that have been approved by the organization and have proper encryption. |
| **P2P** | Block + log | Block + log | |
| Policy Settings | | | |
| **Logging** | Send logs to SafeGuard PortProtector Server<br>Send logs every 12 hours<br>Log connect and disconnect events | Send logs to SafeGuard PortProtector Server<br>Send logs every 12 hours<br>Log connect and disconnect events | Logs should clearly not be stored on the endpoint, but instead sent to the SafeGuard PortProtector Server where they can be protected and viewed by the administrator.<br>Other logging settings here provide adequate EPHI protection by ensuring periodic updating of logs on the server without burdening the network; inclusion of connect and disconnect events to allow for analysis of how long a device was connected; |
| **End-user messages** | Review the end user messages associated with the SOX setting to ensure they are consistent with your formally documented security policies and security awareness training program. | | It is important to provide a constant reminder to system users that they are responsible for protecting the network and sensitive information and complying with policies. Modifying the end-user messages to specifically mention SOX security will assist in the security awareness of your organization. |

| Setting | Standard SOX Approach | Aggressive SOX Approach | Rationale |
|---|---|---|---|
| **Encryption** | Do not allow users to access encrypted devices at home<br><br>Approve read only access for non-encrypted devices. | Do not allow users to access encrypted devices at home<br><br>Approve read only access for non-encrypted devices. | It is important to restrict the use of EPHI to systems with adequate protection measures. Home computers generally lack HIPAA required security controls.<br><br>Setting read-only for non-encrypted devices allows the flexibility of importing information without exposing EPHI to the risk of disclosure from loss or theft of a non-encrypted device. |
| **Options** | Use a different password from the client administration password to uninstall SafeGuard PortProtector<br><br>Full visibility on endpoints | Use a different password to uninstall SafeGuard PortProtector<br><br>Full visibility on endpoints | In order to enforce the principle of separation of duty and general password security, use a different password for the uninstall process of SafeGuard PortProtector Client than the client administration password.<br><br>Consistent with the advice under “end user messages” it is best to let users know about the protections SafeGuard PortProtector is providing. |

### 14.2.3 Other SafeGuard PortProtector SOX Settings

For the appropriate setting of other SafeGuard PortProtector features and options refer to the *Pre-Requisites for Addressing SOX Compliance Issues* detailed in this document. Specifically, the following SafeGuard PortProtector features should follow the business objectives and the sensitive data environment as defined in *Foundations*, *Considerations*, and *Preparations*.

**Alerts**

SafeGuard PortProtector alerts provide oversight of administrative actions and protection of the SafeGuard PortProtector security functions in case of attempted tampering. The following alert options should be set in order to preserve the security functions provided by SafeGuard PortProtector:

- Log all administrative events Logs all administrative actions and provides oversight of SafeGuard PortProtector administration.
- Alert all tempering events Detects tempering attempts and ensures the integrity of end point protection controls.

**SafeGuard PortProtector Administration**

SafeGuard PortProtector may be run by a single administrator or an organization may implement additional access control by defining additional administrators to a subset of administrative functions. This is an implementation of role-based access control and should be considered based on the organizations approach as defined in “Preparation 3: Determine Administrative Roles” which can be found under *Preparations* .Among the roles within the sensitive data environment the organization should consider are the following:

- Log Reviewer - Access to all logs and log functions without ability to edit policies.
- Policy Administrator - Access to edit and administer policies without ability to view logs.
- Audit - Read-only access to administrators console without ability to perform any changes.

The setting of these roles should be based on the administration model and approach of the organization and the support needed for incident response and maintenance. Refer to *Pre-Requisites for Addressing SOX Compliance Issues* for more complete instructions for SafeGuard PortProtector implementation preparation.

**Domain Partitioning**

Further access control granularity may be added with the SafeGuard PortProtector domain partitioning feature. The role based access mechanism includes domain partitioning, which allows an administrator role to be limited to a specific group of clients. This feature is useful in establishing the boundaries of the sensitive data environment by restricting the administrator’s access within defined domains. The setting of these roles should be based on the organization’s administration model and approach and the support needed for incident response and maintenance. Refer to *Pre-Requisites for Addressing SOX Compliance Issues* for more complete instructions for the SafeGuard PortProtector implementation preparation.

**Administrative Password Strength**

All passwords that protect system components within the sensitive data environment must comply with the organization’s formally documented password policies. Formally documented security policies are discussed in more detail in “Consideration 1: Policies and Procedures” under *Considerations* section. Based on the organization’s password strength policy, SafeGuard PortProtector administrative password strength criteria should be defined in the SafeGuard PortProtector to enforce organizational policies. Elements of the password strength include minimum length and required character types.

### 14.2.4 Relevant SOX Requirements

| SOX Requirement | | |
|---|---|---|
| P04.6 | Roles and responsibilities | Roles and responsibilities must be defined and communicated throughout the organization. Once create, these roles must be maintained. |
| P04.8 | Responsibility for risk, security | Specific roles must be created for critical tasks that involve risk management for information security and compliance. |
| P04.9 | Data and system ownership | Owner for critical information must be defined and provided with systems that enforce the data classification. |

| | | |
|---|---|---|
| P06.2 | Enterprise IT risk and internal | The IT framework should deliver a minimal risk at a high value (low cost). Reduction of risks should include preventative, detective and corrective measures to protect business assets. |
| PO7.8 | Job change and termination | In the case of a job change, access rights should be redefined such that risks are minimized. |
| PO9.3 | Event identification | Any potential threats to the infrastructure should be identified, together with the potential impact. |
| DS5.4 | User account management | Any IT implementation must contain a logging and monitoring function that provides early detection of unauthorized activities. |
| DS5.6 | Security incident definition | Security incidents must be clearly defined to ensure that the response follows the incident response process. |
| DS5.7 | Protection of security technology | All security related functions must be tamper resistant such that they cannot be bypassed by unauthorized access. |
| DS5.10 | Network security | Information flows to and from networks must be controlled with security techniques and related management procedures. |
| ME2.1 | Monitoring of Internal Control Framework | The IT environment and controls must be continuously monitored. |
| AC18 | Protection of sensitive information during transmission and transport | Controls must be deployed to protect the confidentiality and integrity of sensitive information during transmission and transport. |

# 15 Appendix G – Using SafeGuard PortProtector in a PCI Regulated Organization

## About This Appendix

In order to create protection of cardholder data credit card companies such as VISA International, MasterCard Worldwide, Discover Financial Services, American Express, and JCB issued security compliance requirements to merchants that processed, stored, or transmitted cardholder information. Although each of these security programs was issued by their respective organizations, the programs were similar in terms of protection requirements. In 2004 the Payment Card Industry (PCI) Security Standards Council was formed to create a common set of requirements for credit card processing merchants. The PCI Data Security Standard (DSS) v1.1 contains the current set of requirements for credit card merchants.

Specifically the PCI DSS control objectives ensure that the organization builds and maintains a secure network; protects cardholder data; maintains a vulnerability management program, implements strong access control measures, monitors and tests networks, and maintains an information security policy. Ensuring security at the endpoints within a network that processes cardholder data is one of the issues that must be addressed by PCI organizations.

SafeGuard PortProtector helps you regain control of your endpoints and address data leakage and targeted attack threats. This chapter provides guidance on how to address these threats within a PCI DSS regulated environment.

The first section, *Pre-Requisites for Addressing PCI DSS Compliance Issues*, examines organizational issues and pre-requisites that must be addressed prior to implementing SafeGuard PortProtector security features and settings. It contains the following sub-sections:

- Foundations translates business objectives into a PCI DSS compliant context.
- Considerations describes the information security threats that must be addressed within the context of the established business mission.
- Preparations describes the activities that should be performed before configuring SafeGuard PortProtector for protection

The second section, *SafeGuard PortProtector PCI DSS Settings* section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product. It contains the following sub-sections:

- PCI DSS Policy Settings describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a PCI DSS environment.
- Other SafeGuard PortProtector PCI DSS Settings describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the PCI organization.
- PCI DSS / SafeGuard PortProtector Feature Mapping provides additional advice on how SafeGuard PortProtector helps to meet PCI DSS Security Rule requirements.

## 15.1 Pre-Requisites for Addressing PCI DSS Compliance Issues

SafeGuard PortProtector provides many security features that can address the threats of endpoint security. In order to effectively utilize the capabilities of the product, the PCI DSS regulated organization should take some preliminary actions to must prepare to use SafeGuard PortProtector for PCI DSS compliance.

There are three categories of pre-requisites for effective implementation of SafeGuard PortProtector for PCI DSS compliance. The first category is *Foundations*. Foundations are basic information security program elements that must be in place in order for any compliance effort to move forward. Foundations include the establishment of business mission statements, and roles, responsibilities required to carry them out. The second pre-requisite is *Considerations*. Considerations are specific information security threats that must be addressed within the context of the established business mission. In this case considerations are specific issues regarding the protection of stored cardholder data in light of endpoint security. The third pre-requisite for effective implementation is *Preparations*. Preparations are activities that must be performed prior to installing and configuring a specific technology product such as SafeGuard PortProtector.

### 15.1.1 Foundations

The evaluation of security controls within an organization requires a context of business objectives. For PCI DSS regulated organizations that context is provided by the following set of foundations that translate business objectives into a PCI DSS compliant context for the implementation of technology.

**Foundation 1: Information Security Program**

An information security program consists of dedicated security professionals supported by management with the appropriate scope, authority, and budget to assess information security risks, recommend mitigation techniques and ensure appropriate security risk management of the organization’s assets. A strong information security program will include an identification of reasonable threats to the organization’s assets, a review of the physical, administrative, and technical controls, and the planning and implementation oversight of security controls to bring the security posture to an acceptable assurance level. Any organization responsible for the protection of cardholder data will need a strong baseline of security controls and organizational support to implement PCI DSS requirements.

**Foundation 2: PCI Compliance Project**

Demonstrating compliance with PCI DSS requirements will require internal and external resources sufficient to manage the project, assess current controls, create or revise existing security policies and procedures, and configure or install new information technology. This compliance process will require resources with experience in your organization’s business objectives and current technology infrastructure as well as resources with experience in PCI DSS compliance readiness or assessment. The compliance process can be a demanding one. Recognizing the resource requirements is the first step.

### 15.1.2 Considerations

To enforce the security cardholder data, there are twelve security control objectives that must be met, each with a set of requirements implementing the objective. Prior to embarking on an effort to implement each requirement a PCI DSS organization should first consider several key elements of the upcoming PCI DSS compliance project. Careful consideration of these elements can help an organization avoid several common pitfalls and increase its efficiency in the PCI DSS compliance effort.

**Consideration 1: Data Architecture**

The root of the PCI DSS requirements is the protection of cardholder data and sensitive authentication data. Cardholder data includes the Primary Account Number (PAN), the cardholder's name, the service code, and the expiration date of the card. Sensitive authentication data includes the information on the "full magnetic stripe", the security code (e.g. CVC2), and the PIN for the card. Sensitive authentication data is protected by ensuring that it is never stored. Cardholder data is required to be protected if it is stored, processed, or transmitted within your organization's applications or systems.

Data architecture is the logical arrangement and association of data elements throughout your system. The structure of your data architecture dictates the application of the PCI DSS requirements on your organization. For example, if your network does not distinguish between cardholder data environments and the rest of your network then it could be argued that the entire network is under the PCI DSS requirements. On the other hand, if you have adequate policies and procedures (such as data classification policies), adequate network separation, and well defined cardholder data applications, then you could argue that only portions of your network fall under the PCI DSS requirements.

**Consideration 2: Data Environment Separation**

The PCI DSS requirements apply to all elements of your cardholder data environment. This includes components of the systems such as network components (e.g. switches, routers firewalls, wireless access points, network appliances, and security appliances), servers (e.g. mail servers, proxy servers, web servers, authentication servers, database servers, domain name servers), and applications (custom or commercial, internal or external facing). System components that are properly separated from the cardholder data environment are not required to meet the PCI DSS requirements. Proper network segmentation and other means of data environment separation can establish a proper environment to protect cardholder data and reduce the overall work required to become PCI DSS compliant. Endpoints within cardholder data network segments would need appropriate protection as defined under PCI DSS and detailed in this document.

**Consideration 3: Policies and Procedures**

A security policy is a statement of management's intent for protecting corporate assets from fraud, waste, and abuse. To be compliant with PCI DSS, the organization must have a strong security policy that provides the employees with security awareness and informs them of their responsibilities for protecting the organization's assets. Specifically, PCI DSS requires a security policy address the following relevant areas concerning the implementation of a technology such as SafeGuard PortProtector:

- Technology Usage Policy. A PCI organization is required to have a usage policy for "employee-facing" technology. The organization will require management approval of the SafeGuard PortProtector product and an update to the acceptable use policies regarding the administration of SafeGuard PortProtector.
- Information Security Responsibilities. A PCI organization is required to define and assign information security and security management responsibilities for all employees and contractors. The organization will need to update job descriptions (or other means of assigning security responsibilities) to include the administration of the SafeGuard PortProtector product.
- Formal Awareness Program. A PCI organization is required to implement a formal security awareness program. The introduction of SafeGuard PortProtector to endpoints (i.e. desktops and laptops) will require an update to the user education.

### 15.1.3 Preparations

SafeGuard PortProtector allows organizations to control access and protect endpoints based on user roles, network domains, computer types, and systems and data sensitivity. The specific implementation and configuration of SafeGuard PortProtector requires an accurate knowledge of objects SafeGuard PortProtector is to protect, the policies it is to enforce, and the administrative roles that will maintain the SafeGuard PortProtector software. The following activities are an important element of the preparation to install and configure SafeGuard PortProtector for the protection of cardholder data.

**Preparation 1: Determine Endpoint Protection Needs**

SafeGuard PortProtector provides the ability to protect stored cardholder data for uncontrolled export on removable devices at endpoints. On the other hand your organization has a variety of business needs that will require connectivity to external storage devices, wireless networks, and other possible threats. In preparation for a SafeGuard PortProtector deployment your organization should determine the protection and business needs of the endpoints.

**Instructions:**

- Update endpoint inventory and classification. Be sure that you are aware of all endpoints within your network that store, process, or transmit cardholder data. This can be done through a manual inventory process of through the use of directory services. Classification is based on your data classification policy and includes a classification of endpoints that handle cardholder data.
- Scan each endpoint to detect port, device, and Wi-Fi usage. The SafeGuard PortAuditor utility will automatically detect devices and networks that are currently or previously connected.
- Review your security policies and procedures, specifically as they address security design principles such as "Default – No Access" and "Least Privilege". These policies and procedures should be applied to the endpoints that have now been inventoried, classified, and scanned. Make a list of the intended profiles for each endpoint classification.

**Preparation 2: Determine User Access Roles**

SafeGuard PortProtector allows for the specification of allowed ports, devices, and Wi-Fi usage according to user, user group, or organizational unit as defined by Active Directory or Novel eDirectory. It is important to note that any user privileges granted through this mechanism will trump those specified for an individual endpoint. For example, if you set up a user to have Wi-Fi access (over WPA networks) and have also locked down a laptop to block Wi-Fi access, that user will be able to gain Wi-Fi access through that laptop. With this rule in mind it is strongly recommended that you be very careful when creating any user privileges as those privileges will apply to any endpoint to into which that user logs.

**Instructions:**

- Determine user roles within your SafeGuard PortProtector implementation.
- User – this role is the normal user role that has no additional privileges associated.
- Privileged user – this role has extended privileges such as the use of a specifically permitted non-encrypting device.
- Determine compensating controls placed on privileged users.
- Logs and alerts – at a minimum plan to set privilege user policies to log allowed behavior that is extended from the normal user role. Consider setting alerts on highly sensitive behavior such as the use of a specifically permitted non-encrypting device.

**Preparation 3: Determine Administration Roles**

SafeGuard PortProtector allows for multiple administration roles according to privilege and domain. The use of these administrative role options should be determined prior to installation of SafeGuard PortProtector.

**Instructions:**

- Determine if your implementation of SafeGuard PortProtector will follow a centralized or de-centralized administration model.
- Centralized – a single entity is responsible for the administration of SafeGuard PortProtector .
- De-centralized – administration of SafeGuard PortProtector is delegated to departments that are responsible for the administration of their own domain. If you chose this method of administration, then determine the domain partitions for which each department will be responsible for the administration.
- Determine administration roles within each domain.
- The SafeGuard PortProtector administrator may be set up as a single role or you may delegate administrative privileges to implement separation of duties. Determine the set of administrative roles that you will implement.
- Plan maintenance and incident response function for SafeGuard PortProtector administration.
- Incident response – those responsible for responding to incidents involving lost or stolen storage devices, rogue networks, hybrid network bridging, or unapproved data removal will require special permissions within SafeGuard PortProtector and access to audit tools. Document the incident response roles within your organization and the permissions and access required.
- Maintenance – those responsible for handling end user issues such as peripherals and network connectivity will require the ability to request modifications to object or user permissions. Document maintenance roles within your organization and the permissions and access required.

## 15.2 SafeGuard PortProtector PCI DSS Settings

This section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product.

- PCI DSS Policy Settings describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a PCI DSS environment.
- Other SafeGuard PortProtector PCI DSS Settings describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the PCI organization.
- PCI DSS / SafeGuard PortProtector Feature Mapping provides additional advice on how SafeGuard PortProtector helps to meet PCI DSS Security Rule requirements.

### 15.2.1 PCI DSS Policy Settings

The following table is a guide to the SafeGuard PortProtector administrator in the setting and configuration of SafeGuard PortProtector for implementation within a cardholder data environment. Many of the settings below are a direct implementation of a specific PCI DSS requirement, while others follow good security practices consistent with the level of security achieved through the other PCI DSS requirements. The PCI DSS settings are to be used as guidelines for setting the parameters of SafeGuard PortProtector and not to be interpreted as additional PCI DSS requirements.

| Setting | PCI Setting | Rationale |
|---|---|---|
| **Policy** | | Create new policies based on the built-in policy of PCI DSS. Each policy can then be modified as determined by the compliance officer and in accordance with the organization's business objectives. |
| **Port Control:** | | |
| **USB** | Restrict | Restricting access to these ports allows for a finer granularity of control under the device control section of the policy-security. |
| **FireWire** | Restrict | |
| **PCMCIA** | Restrict | |
| **SD** | Allow | Allowing access to these ports is required for some standard human interface devices. The access restrictions to these ports for storage devices will be further restricted through storage control below. |
| **Serial** | Allow | |
| **Parallel** | Allow | |
| **WiFi** | Restrict | Restricting access to Wi-Fi networks allows for a finer granularity of control under the Wi-Fi control section of the policy-security. |
| **Modem** | Allow + log | Use of Modem can lead to unauthorized network connections but may be a common business use. At a minimum use of these devices should be logged. |
| **IrDA** | Block + log | |
| **Bluetooth** | Block + log | |

| Setting | PCI Setting | Rationale |
|---|---|---|
| **Network Bridging** | Block (All) | |
| Device Control | | |
| **Hardware Keyloggers** | Allow | Although the use of hardware keyloggers should be restricted and users should be protected from these attacks, usability concerns override the need for this restriction. |
| **Human Interface** | Allow | It is typically not considered a risky practice to allow users to connect to human interface devices such as keyboards and mice |
| **Printers** | Allow + log | Although a printer can be a data leakage source, printing is a common user function within most organizations. This risk can be mitigated by physical and administrative controls. |
| **PDA** | Restrict, white list, log | PDAs, mobile phones, Imaging devices (such as scanners) and Audio / Video devices (such as MP3 players) present a clear risk to the control and protection of cardholder data. The use of such devices should be blocked. |
| **Mobile Phones** | | |
| **Imaging** | | |
| **Audio / video Devices** | | |
| **Network Adapters** | Allow | Network adapters allow the PC to be connected to a network. This is a common configuration and should not be blocked or logged. |
| **Smart Cards** | Allow | Smart Cards are common as an authentication device. They do not pose a reasonable threat to cardholder data. |
| **Content security devices** | Allow | Content security devices monitor the content of the flow of data to and from the endpoint. If such devices are present they are part of a solution to enforce security and should not be blocked at the endpoint. |
| **Unclassified devices** | Block + Log | Unclassified devices are any devices that are not otherwise specified. These should not turn up very often, and present a clear risk to the protection of cardholder data. |
| Storage Control | | |
| **Autorun function** | Block | A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default. |

| Setting | PCI Setting | Rationale |
|---|---|---|
| **Removable storage** | Encrypt + log<br><br>block smart function | Storage devices (such as USB drives) present a clear risk to the protection of cardholder data. The organization should limit the use of storage devices to approved devices with the ability to appropriately encrypt the data. Use of these devices should be logged.<br><br>A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default.<br><br>Certain formats for writing files to media such as CD or DVD do not support the event logging. To preserve the logging settings for all files the "block unsupported burning formats" option should remain checked. |
| **External HD** | Encrypt + log | |
| **CD/DVD** | Encrypt + log<br><br>block unsupported burning formats | |
| **Floppy Drives** | Read only + log | |
| **Tape Drives** | Block + log | |
| **File Control** | Log – write only | In order to support audit and investigation of security incidents involving cardholder data, the organization should log all files written to external storage devices. |
| **WiFi Network** | Restrict, white list WPA encrypted networks, log | Wireless networks present a clear risk to the control and protection of cardholder data. At a minimum an organization should log any such behavior. Any use of Wi-Fi networks should be logged and limited to an approved list of Wi-Fi networks with proper encryption. |
| **P2P** | Block + log | |
| Policy Settings | | |
| **Logging** | Send logs to SafeGuard PortProtector Server<br><br>Send logs every 12 hours<br><br>Log connect and disconnect events | Logs should clearly not be stored on the endpoint, but instead sent to the SafeGuard PortProtector Server where they can be protected and viewed by the administrator.<br><br>Other logging settings here provide adequate cardholder protection by ensuring periodic updating of logs on the server without burdening the network; inclusion of connect and disconnect events to allow for analysis of how long a device was connected. |
| **End-user messages** | Review the end user messages associated with the PCI setting to ensure they are consistent with your formally documented security policies and security awareness training program. | It is important to provide a constant reminder to those exposed to cardholder data that they are responsible for protecting cardholder data and complying with policies. Modifying the end-user messages to specifically mention PCI security and cardholder data protection will assist in the security awareness of your organization. |

| Setting | PCI Setting | Rationale |
|---|---|---|
| **Encryption** | Do not allow users to access encrypted devices at home<br><br>Approve read only access for non-encrypted devices | It is important to restrict the use of cardholder to systems with adequate protection measures. Home computers would generally fall outside of the cardholder data environment and should not have the ability to read cardholder data.<br><br>Setting read-only for non-encrypted devices allows the flexibility of importing information without exposing cardholder data to the risk of disclosure from loss or theft of a non-encrypted device. |
| **Options** | Use a different password to uninstall SafeGuard PortProtector<br><br>Full visibility on endpoints | In order to enforce the principle of separation of duty and general password security, use a different password for the uninstall process of SafeGuard PortProtector Client than the client administration password.<br><br>Consistent with the advice under “end user messages” it is best to let users know about the protections SafeGuard PortProtector is providing to PCI security. |

## 15.2.2 Other SafeGuard PortProtector PCI DSS Settings

For the appropriate setting of other SafeGuard PortProtector  features and options refer to the *Pre-Requisites for Addressing PCI DSS Compliance Issues* detailed in part 1 of the PCI DSS Compliance with SafeGuard PortProtector  document. Specifically, the following SafeGuard PortProtector features should follow the business objectives and the cardholder data environment as defined in *Foundations*, *Considerations*, and *Preparations*.

**Alerts**

SafeGuard PortProtector alerts provide oversight of administrative actions and protection of the SafeGuard PortProtector  security functions in case of attempted tampering. The following alert options should be set in order to preserve the security functions provided by SafeGuard PortProtector :

- Log all administrative events - Logs all administrative actions and provides oversight of SafeGuard PortProtector administration.
- Alert all tempering events - Detects tempering attempts and ensures the integrity of end point protection controls.

**SafeGuard PortProtector  Administration**

SafeGuard PortProtector may be run by a single administrator or an organization may implement additional access control by defining additional administrators to a subset of administrative functions. This is an implementation of role-based access control and should be considered based on the organizations approach as defined in “Preparation 3: Determine Administrative Roles” under *Preparations* section. Among the roles within the cardholder data environment the organization should consider are the following:

- Log Reviewer -Access to all logs and log functions without ability to edit policies.

- Policy Administrator - Access to edit and administer policies without ability to view logs.
- Audit - Read-only access to administrators console without ability to perform any changes.

The setting of these roles should be based on the administration model and approach of the organization and the support needed for incident response and maintenance. Refer to *Pre-Requisites for Addressing PCI DSS Compliance Issues* for more complete instructions for SafeGuard PortProtector implementation preparation.

**Domain Partitioning**

Further access control granularity may be added with the SafeGuard PortProtector domain partitioning feature. The role based access mechanism includes domain partitioning, which allows an administrator role to be limited to a specific group of clients. This feature is useful in establishing the boundaries of the cardholder data environment by restricting the administrator's access within defined domains. The setting of these roles should be based on the organization's administration model and approach and the support needed for incident response and maintenance. Refer to *Pre-Requisites for Addressing PCI DSS Compliance Issues* for more complete instructions for the SafeGuard PortProtector implementation preparation.

**Administrative Password Strength**

All passwords that protect system components within the cardholder data environment must comply with the organization's formally documented password policies and PCI DSS requirement 8.5. Formally documented security policies are discussed in more detail in "Consideration 1: Policies and Procedures" under *Considerations* section. Required elements of the password strength include a minimum length of seven (7) characters, at least one (1) character, and at least one (1) number.

## 15.2.3 PCI DSS / SafeGuard PortProtector Feature Mapping

SafeGuard PortProtector provides PCI DSS organizations additional technical controls to protect cardholder data at system endpoints and address data leakage and targeted attack threats. As discussed throughout this document SafeGuard PortProtector can address data leakage risks, targeted attack threats, and many of the PCI DSS requirements. Although obvious, it should be noted that SafeGuard PortProtector provides a portion of the control objectives necessary for complete PCI DSS compliance. The table below provides additional advice on how SafeGuard PortProtector helps to meet PCI DSS requirements.

| PCI | | | |
|---|---|---|---|
| Requirement Number | Requirement Description | Relevant SafeGuard PortProtector Features | How to Satisfy PCI DSS Controls with SafeGuard PortProtector |
| 2 | Do not use vendor-supplied defaults for system passwords and other security parameters. | SafeGuard PortProtector provides administrators the ability to change passwords (including the default password). | Change the default administration and install passwords for SafeGuard PortProtector. |

<table>
<tr><td>2.1</td><td>Always change vendor-supplied defaults before installing a system on the network.</td><td></td><td></td></tr>
<tr><td>2.2.2</td><td>Disable all unnecessary and insecure services and protocols….</td><td rowspan="2">SafeGuard PortProtector provides the ability to block access to unnecessary ports and storage devices that may pose a threat to cardholder data.</td><td rowspan="2">Use the SafeGuard PortProtector recommended settings for port, device, storage, file, and Wi-Fi network control to block or restrict access to unnecessary devices. [See recommended settings in table above.]</td></tr>
<tr><td>2.2.4</td><td>Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.</td></tr>
<tr><td>4.1.1</td><td>For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology…..</td><td>SafeGuard PortProtector allows the organization to create policies that force the use of encrypted Wi-Fi channels for secure transfer of data. These policies can even be set to require a specific level of encrypted (e.g. WPA).</td><td>Under port control, restrict Wi-Fi networks. Under Wi-Fi networks set a white list of approved Wi-Fi networks to WPA encrypted networks.</td></tr>
<tr><td>8</td><td>Assign a unique ID to each person with computer access</td><td rowspan="3">SafeGuard PortProtector provides the ability to unique user IDs for all administrative users.</td><td rowspan="3">For all SafeGuard PortProtector administrative accounts assign a single account to a single user – no group administration accounts.<br><br>Set password complexity to a minimum of seven (7) characters and at least one number and at least one letter.</td></tr>
<tr><td>8.1</td><td>Identify all users with a unique user name before allowing them to access system components or cardholder data.</td></tr>
<tr><td>8.2</td><td>In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: (Password, Token devices, Biometrics)</td></tr>
</table>

| 9 | Restrict physical access to cardholder data | SafeGuard PortProtector can be applied to network endpoints to restrict data leakage or unintended data transfers between systems. PCI organizations must limit system components that require access, transmission, or storage of cardholder data and physically separate these from other network components. | See “Consideration 2: Data Environment Separation” for a discussion of separating the cardholder data environment. |
|---|---|---|---|
| 10 | Track and monitor all access to network resources and cardholder data | SafeGuard PortProtector records endpoint events associated with storage devices and media in client logs. An event may be a device connection or disconnection, a wireless network connection, tampering attempts or administrator login. Event logs include endpoint identify, user, event type, and time. SafeGuard PortProtector also creates server logs for administrative events such as administrator login, publishing policies and performing backups. | Use the SafeGuard PortProtector recommended logging settings for port, device, storage, file, and Wi-Fi network control to block or restrict access to unnecessary devices. [See recommended settings in table above.]<br><br>Log all administrative events and alert to all tempering events. |
| 10.2 | Implement automated audit trails for all system components to reconstruct the following events:<br>Individual user accesses to cardholder data<br>All actions taken by any individual with administrative privileges<br>Access to all audit trials<br>Invalid logical access attempts<br>Use of identification and authentication mechanisms<br>Initialization of the audit logs. | | |

| | | | |
|---|---|---|---|
| 10.3 | Record at least the following audit trail entries for all system components for each event:<br>User identification<br>Type of event<br>Data and time<br>Success or failure indication<br>Origin of event<br>Identity or name of affected data, system component, or resource. | | |
| 10.4 | Synchronize all critical system clocks and times | SafeGuard PortProtector audit log timestamps are based on the system time of the endpoint. | Audit log timestamps are a built-in function of SafeGuard PortProtector. To synch system clocks, apply controls such as network time protocol to the desktop. |
| 10.5 | Secure audit trails so they cannot be altered. | Client and Server logs are sent to a log repository and stored on the Management Server at the defined intervals. | Use the SafeGuard PortProtector recommended settings for logging: |
| 12 | Maintain a policy that addresses information security for employees and contractors. | SafeGuard PortProtector is a technology control that can implement policies and procedures to prevent and detect security violations at the network endpoints. | See consideration 3 [Policies and Procedures] for instructions on what policies and procedures need to be implemented. |

# 16 Appendix H – Using SafeGuard PortProtector in a FISMA Regulated Organization

## About This Appendix

The E-Government Act (Public Law 107-347) passed by the 107th US Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

SafeGuard PortProtector helps you control your endpoints and address data leakage and targeted attack threats. This chapter provides guidance on how to address these threats within a FISMA-regulated environment.

The first section Pre-Requisites for Addressing FISMA Compliance Issues, examines organizational issues and pre-requisites that must be addressed prior to implementing SafeGuard security features and settings. It contains the following sub-sections:

- Foundations translates operational objectives into a FISMA compliant context.
- Considerations describes the information security threats that must be addressed within the context of the established mission requirements.
- Preparations describes the activities that should be performed before configuring SafeGuard for protection.

The second section, Implementing SafeGuard PortProtector in a FISMA Regulated Organization, provides specific Sophos setting guidance for the policy, user, and administrator parameters within the Sophos solution. It contains the following sub-sections:

- FISMA policy settings describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a FISMA environment.
- Other SafeGuard FISMA Settings describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to operational objectives and the environment of the FISMA organization.
- FISMA/SafeGuard PortProtector Feature Mapping provides additional advice on how SafeGuard PortProtector helps to meet FISMA Security Rule requirements.

## 16.1 Pre-Requisites for Addressing FISMA Compliance Issues

SafeGuard PortProtector provides many security features that can address the threats of endpoint security. In order to effectively utilize the capabilities of the product, the FISMA regulated organization should take some preliminary actions to prepare to use SafeGuard PortProtector for FISMA 404 compliance.

There are three categories of pre-requisites for effective implementation of SafeGuard PortProtector for FISMA compliance. The first category is Foundations. Foundations are basic information security program elements that must be in place in order for any compliance effort to move forward. Foundations include the establishment of mission statements, and roles, responsibilities required to carry them out. The second pre-requisite is Considerations. Considerations are specific information security threats that must be addressed within the context of the established objectives. The third pre-requisite for effective implementation is Preparations. Preparations are activities that must be performed prior to installing and configuring a specific technology product such as SafeGuard PortProtector.

### 16.1.1 Foundations

The evaluation of security controls within an organization requires a context of operational objectives. For FISMA regulated organizations that context is provided by the following set of foundations that translate mission objectives into a FISMA compliant context for the implementation of technology.

**Foundation 1: Information Security Program**

An information security program consists of dedicated security professionals supported by management with the appropriate scope, authority, and budget to assess information security risks, recommend mitigation techniques and ensure appropriate security risk management of the organization’s assets. A strong information security program will include an identification of reasonable threats to the organization’s assets, a review of the physical, administrative, and technical controls, and the planning and implementation oversight of security controls to bring the security posture to an acceptable assurance level.

**Foundation 2: FISMA Compliance Project**

Demonstrating compliance with FISMA baseline requirements will require internal and external resources sufficient to manage the project, assess current controls, create or revise existing security policies and procedures, and configure or install new information technology. This compliance process will require resources with experience in your organization’s mission objectives and current technology infrastructure as well as resources with experience in FISMA compliance readiness or assessment. The compliance process can be a demanding one. Recognizing the resource requirements is the first step.

### 16.1.2 Considerations

To ensure the protection of the organization’s assets there are a number of control objectives that must be met. Prior to embarking on an effort to implement these control objectives, the FISMA organization should first consider several key elements of the upcoming FISMA compliance project. Careful consideration of these elements can help an organization avoid several common pitfalls and increase its efficiency in the FISMA compliance effort.

**Consideration 1: Risk Assessment**

The basic step of any information security policy is to determine which information needs to be protected, and which personnel, systems and devices may or may not be granted access to it. A comprehensive risk assessment plan should be based upon, or include a detailed review and categorization of confidential information in the organization according to risk levels. Based on outcome of the risk assessment procedure, it will be possible to determine the proper security controls needed to protect confidential information and information systems.

**Instructions:**

- Review the threats facing information systems in the organization, and the channels through which information might leak out of the organization. Assess the potential damage and harm that may result from unauthorized access, disclosure, or loss of such information.
- Create an inventory of all peripheral devices used by your organization, and specifically of all storage and storage-enabled device (such as smart phones, media players, etc).
- Determine which systems, personnel, and peripheral devices may access confidential information, and how they may be used inside and outside of the organization.

**Consideration 2: Policies and Procedures**

A security policy is a statement of management's intent for protecting corporate assets from fraud, waste, and abuse. With the emergence of the data leakage threat data access policies and procedures must be reviewed and revised. The principle of least privilege, which states that each user should have only the level of access required to perform their job, needs to be interpreted to address portable media and devices.

**Instructions:**

- Ensure that your current policies are based on the principle of "Default – No Access". This principle dictates that by default all users have no access to any corporate resources. If no such policy statement exists – create one.
- Develop a guidance policy that interprets the "Default – No Access" policy for the roles within your organization and to the computing devices within your organization.
- Develop procedures for handling exceptions to the "Default – No Access" policy. These exceptions will be based on operational needs such as media backup, data transfer, and remote access to networks for telecommuting. Each procedure should address the risk through compensating controls such as policy, sanctions, asset tracking, multi-factor authentication, oversight, and encryption.

**Consideration 3: Training**

Effective security awareness and training is an important element of asset protection. Information security training programs need to be periodically updated to reflect changes in threats and organizational policies. A project to update security awareness and training programs should be part of the overall data leakage risk mitigation project.

**Instructions:**

Update annual security awareness training and periodic security awareness reminders to include a discussion of data leakage threats, updated policies, required user actions, prohibited behavior, and restricted devices.

- Wi-Fi Threats: use on unapproved networks, rogue networks, hybrid network bridging, WEP authentication.
- Mobile/Storage Device Threats: physical loss, data removal, malicious code insertion.

**Consideration 4: Incident Response**

In the event of a security breach resulting in the disclosure, modification, or interruption of service, FISMA compliant organizations are required to have policies, procedures, and the capability of investigating the incident. As the set of possible security incidents expands to include data leakage, organizations must update their policies, procedures, and capabilities to respond to these incidents.

**Instructions:**

Update the incident response procedures to address data leakage issues. Specifically, create procedures for the following incident types.

- Lost or stolen mobile/storage device
- Found rogue network
- Found hybrid network bridging
- Unapproved data removal

### 16.1.3 Preparations

SafeGuard PortProtector enables organizations to control access and protect endpoints based on user roles, network domains, computer types, and criticality of systems and data. The specific implementation and configuration of SafeGuard PortProtector requires an accurate knowledge of the objects SafeGuard PortProtector is to protect, the policies it is to enforce, and the administrative roles that will be used to maintain the SafeGuard PortProtectorsoftware. The following activities are an important part of the preparation to install and configure SafeGuard PortProtector for the implementation of appropriate internal controls.

**Preparation 1: Determine Endpoint Protection Needs**

SafeGuard PortProtector provides the ability to protect stored data for uncontrolled export on removable devices at endpoints. On the other hand your organization has a variety of operational needs that will require connectivity to external storage devices, wireless networks, and other possible threats. In preparation for a SafeGuard PortProtector deployment your organization should determine the protection and operational needs of the endpoints.

**Instructions:**

- Update endpoint inventory and classification. Be sure that you are aware of all the endpoints within your network that store, process, or transmit sensitive data. This can be done through a manual inventory process or through the use of directory services. Classification is based on your data classification policy and includes a classification of endpoints that handle sensitive data.
- Scan each endpoint to detect port, device, and Wi-Fi usage. The SafeGuard Auditor utility will automatically detect devices and networks that are currently or previously connected.
- Review your "Default – No Access" and least privilege policies, as they apply to the endpoints that have now been inventoried, classified, and scanned. Make a list of the intended profiles for each endpoint classification.

**Preparation 2: Determine User Access Roles**

SafeGuard PortProtector allows specifing the allowed ports, devices, and Wi-Fi usage according to user, user group, or organizational unit as defined by Active Directory or Novel eDirectory. It is important to note that any user privileges granted through this mechanism will trump those specified for an individual endpoint. For example, if you set up a user to have Wi-Fi access (over WPA networks) and also have locked down a laptop to block Wi-Fi access, that user will be able to gain Wi-Fi access through that laptop. With this rule in mind it is strongly recommended that you be very careful when creating any user privileges, since these privileges will apply to any endpoint into which that user logs.

**Instructions:**

- Determine user roles within your SafeGuard PortProtector implementation.
- User – this role is the normal user role that has no additional privileges associated.
- Privileged user – this role has extended privileges such as the ability to write files to a USB device or connect to a WPA-enabled Wi-Fi network.
- Determine compensating controls placed on privileged users.
- Logs and alerts – at the minimum, plan to set privileged user policies to log allowed behavior that is extended from the normal user role. Consider setting alerts on highly sensitive behavior such as connecting to external hard drives.

**Preparation 3: Determine Administration Roles**

SafeGuard PortProtector allows for multiple administration roles according to privilege and domain. The use of these administrative role options should be determined prior to installation of SafeGuard PortProtector.

**Instructions:**

- Determine if your implementation of SafeGuard PortProtector will follow a centralized or de-centralized administration model.
- Centralized – a single entity is responsible for the administration of SafeGuard PortProtector.
- De-centralized – administration of SafeGuard PortProtector is delegated to departments that are responsible for the administration of their own domain. If you chose this method of administration, then determine the domain partitions for each department which will be responsible for the administration.
- Determine administration roles within each domain.

- The SafeGuard PortProtector administrator may be set up as a single role or you may delegate administrative privileges to implement separation of duties. Determine the set of administrative roles that you will implement.
- Plan maintenance and incident response function for SafeGuard PortProtector administration.
- Incident response – those responsible for responding to incidents involving lost or stolen storage devices, rogue networks, hybrid network bridging, or unapproved data removal will require special permissions within SafeGuard PortProtector and access to auditing tools. Document the incident response roles within your organization and the permissions and access required.
- Maintenance – those responsible for handling end user issues such as peripherals and network connectivity will require the ability to request modifications to object or user permissions. Document maintenance roles within your organization and the permissions and access required.

## 16.2 Implementing SafeGuard PortProtector in a FISMA Regulated Organization

This section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product.

- FISMA policy settings, describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a FISMA regulated environment.
- Other SafeGuard PortProtector FISMA Settings, describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy.
- FISMA/SafeGuard PortProtector Feature Mapping, provides additional information on the FISMA Security Rule requirements.

### 16.2.1 FISMA policy settings

The following table is a guide for the SafeGuard PortProtector administrator in the setting and configuration of SafeGuard PortProtector for implementation within a FISMA regulated environment. SafeGuard PortProtector provides organizations with additional technical controls to protect cardholder data at system endpoints and address data leakage and targeted attack threats. As discussed throughout this appendix, SafeGuard PortProtector can address data leakage risks, targeted attack threats, and many of the FISMA requirements.

| Setting | FISMA Setting | Rationale |
|---|---|---|
| **Policy** | | Create new policies based on the built-in policy of FISMA best practices. Each policy can then be modified as determined by the compliance officer and in accordance with the organization's operational needs. |
| **Port Control:** | | |
| **USB** | Restrict | Restricting access to these ports allows for a finer granularity of control under the device control section of the policy-security. |
| **FireWire** | Restrict | |
| **PCMCIA** | Restrict | |
| **SD** | Allow | Any storage-capable devices connected to this port will be allowed or blocked based on the permissions defined by storage device settings. |
| **Serial** | Allow | Allowing access to these ports is required for some standard human interface devices. |
| **Parallel** | Allow | |
| **WiFi** | Restrict | Restricting access to Wi-Fi networks allows for a finer granularity of control under the Wi-Fi control section of the policy-security. |
| **Modem** | Allow + log | Use of a modem can lead to unauthorized network connections but may have a common business use. At the minimum, however, use of these devices should be logged. |
| **IrDA** | Block + log | Use of IrDA or Bluetooth can lead to unauthorized network connections. Use of these devices should be blocked and logged. |
| **Bluetooth** | Block + log | |
| **Network Bridging** | Block (All) | Blocking user access to Wi-Fi, Bluetooth, modems, and IrDA links while connected to the TCP/IP network interface, protects endpoints from the dangerous practice of hybrid network bridging. |
| **Device Control:** | | |
| **Hardware Keyloggers** | Allow | Although the use of hardware keyloggers should be restricted and users should be protected from these attacks, usability concerns override the need for this restriction. |
| **Human Interface** | Allow | It is typically not considered risky to allow users to connect to human interface devices, such as keyboards and mice. |
| **Printers** | Allow + log | Although a printer can be a data leakage source, printing is a common user function within most organizations. This risk can be mitigated by physical and administrative controls. |
| **PDA** | Restrict, white list, log | PDAs, mobile phones, imaging devices (such as scanners) and audio/video devices (such as MP3 players) present a clear risk to the control and protection of confidential data. The use of such devices should be blocked. |
| **Mobile Phones** | | |
| **Imaging** | | |

| Setting | FISMA Setting | Rationale |
|---|---|---|
| **Audio/ video Devices** | | Where required, the use of allowed devices is approved by device whitelist groups. Whitelists can be created based on vendor ID, product ID, or device serial number. |
| **Network Adapters** | Allow | Network adapters allow the computer to be connected to a network. This is a common configuration and should not be blocked or logged. |
| **Smart Cards** | Allow | Smart Cards are commonly used as authentication devices. They do not pose a reasonable threat to network security. |
| **Content security devices** | Allow | Content security devices monitor the content of the flow of data to and from the endpoint. If such devices are present, they are usually part of a solution to enforce security and should not be blocked at the endpoint. |
| **Un-classified devices** | Block + Log | Unclassified devices are any devices that are not otherwise specified. These should not turn up very often, and present a clear risk to the confidential data. |
| **Storage Control:** | | |

| Setting | FISMA Setting | Rationale |
|---|---|---|
| **Autorun function** | Block | A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat frequently used by malware and should be disabled by default. |
| **Removable storage** | Encrypt + log<br>Apply File Control on files written to storage devices<br>Apply File Control on Files Read from storage devices<br>block smart functionality | Storage devices (such as USB drives) present a clear risk to confidential data. The organization should limit the use of storage devices to approved devices with the ability to appropriately encrypt the data. Use of these devices should be logged.<br>A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default. |
| **External HD** | Encrypt + log | |
| **CD/DVD** | Encrypt + log<br>Apply File Control on files written to storage devices<br>Apply File Control on Files Read from storage devices<br>Block unsupported burning formats | Certain formats for writing files to media such as CD or DVD do not support file logging. To preserve the logging settings for all files the "block unsupported burning formats" option should remain checked. |
| **Floppy Drives** | Read only + log | Because reading data from floppy disks is sometimes still required, the system allows read-only capability for such media. |
| **Tape Drives** | Block + log | As most users rarely use tape drives in their daily work, if at all, this option is blocked by default. |
| **File Control** | Log – write only | In order to support audit and investigation of security incidents involving confidential data, the organization should log all files written to external storage devices. |
| **WiFi Network** | Restrict, white list WPA encrypted networks, log | Wireless networks present a clear risk to the control and protection of confidential data. At the minimum, an organization should log any such behavior. Any use of Wi-Fi networks should be logged and limited to an approved list of Wi-Fi networks with proper encryption. |
| **P2P** | Block + log | |
| **Policy Settings** | | |

| Setting | FISMA Setting | Rationale |
|---|---|---|
| **Logging** | Send logs to SafeGuard PortProtector Server<br>Send logs every 12 hours<br>Log connect and disconnect events | Logs should clearly not be stored on the endpoint, but instead sent to the SafeGuard PortProtector Server where they can be protected and viewed by the administrator.<br>Other logging settings here provide adequate protection by ensuring periodic updating of logs on the server without burdening the network; inclusion of connect and disconnect events to allow for analysis of how long a device was connected. |
| **End-user messages** | Review the end user messages associated with the FISMA settings to ensure that they are consistent with your formally documented security policies and security awareness training program. | It is important to provide a constant reminder to personnel exposed to confidential data that they are responsible for protecting data and complying with policies. Modifying the end-user messages to specifically mention FISMA security and will assist in the security awareness of your organization. |
| **Media Encryption** | Do not allow users to access encrypted devices on computers outside of the network.<br>Approve read only access for non-encrypted devices. | Using encrypted storage devices outside of the organization (at home or on external networks) poses a security threat of data leakage through unsecured networks.<br>Setting read-only for non-encrypted devices allows the flexibility of importing information from removable storage devices without exposing confidential data to the risk of disclosure from loss or theft of a non-encrypted device. |

### 16.2.2 Other SafeGuard PortProtector FISMA Settings

For the appropriate setting of other SafeGuard PortProtector features and options refer to the Pre-Requisites for Addressing FISMA Compliance Issues detailed in this document. Specifically, the following SafeGuard PortProtector features should follow the business objectives and the sensitive data environment, as defined in Foundations, Considerations, Preparations.

**Logging of System Events**

SafeGuard PortProtector alerts provide supervision of administrative actions and protection of the SafeGuard PortProtector security functions in case of attempted tampering. The following alert options should be set in order to preserve the security functions provided by SafeGuard PortProtector:

- Log all administrative events, logs all administrative actions and provides supervision of SafeGuard PortProtector administration.
- Alert all tampering events, detects tampering attempts and ensures the integrity of endpoint protection controls.

**SafeGuard PortProtector Administration**

SafeGuard PortProtector can be run by a single administrator or an organization may implement additional access control by defining additional administrators to a subset of administrative functions. This is an implementation of role-based access control and should be considered based on the organizations approach as defined in “Preparation 3: Determine Administrative Roles” which can be found under Preparations. Among the roles within the sensitive data environment the organization should consider are the following:

- Log Reviewer - Access to all logs and log functions, without the ability to edit policies.
- Policy Administrator - Access to edit and administer policies, without the ability to view logs.
- Audit - Read-only access to the administrators console, without the ability to perform any changes.

The setting of these roles should be based on the administration model and approach of the organization and the support needed for incident response and maintenance. Refer to Pre-Requisites for Addressing FISMA Compliance Issues for more complete instructions about SafeGuard PortProtector implementation preparation.

**Domain Partitioning**

Further access control granularity may be added with the SafeGuard PortProtector domain partitioning feature. The role-based access mechanism includes domain partitioning, which allows an administrator’s role to be limited to a specific group of clients. This feature is useful in establishing the boundaries of the sensitive data environment by restricting the administrator’s access within defined domains. The setting of these roles should be based on the organization’s administration model and approach and the support needed for incident response and maintenance. Refer to Pre-Requisites for Addressing FISMA Compliance Issues for more complete instructions about SafeGuard PortProtector implementation preparation.

**Administrative Password Strength**

All passwords that protect system components within the sensitive data environment must comply with the organization’s formally documented password policies. SafeGuard PortProtector Administrative Password strength rules apply passwords of all SafeGuard PortProtector administrators to the SafeGuard PortProtector Management Console, uninstall passwords of endpoint clients, and user passwords on encrypted devices.

Formally documented security policies are discussed in more detail in “Consideration 1: Policies and Procedures” in the Considerations section. Based on the organization’s password strength policy, SafeGuard PortProtector administrative password strength criteria should be defined in the SafeGuard PortProtector to enforce organizational policies. Elements of the password strength include minimum length and required character types.

### 16.2.3 FISMA/SafeGuard PortProtector Feature Mapping

The following table provides a list of relevant FISMA requirements, and maps the relevant corresponding SafeGuard PortProtector features, and brief instructions on how to apply them. The full FISMA requirements list (updated to August 2009) can be found at the following link: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

| Requirement Number | Requirement Description | Relevant SafeGuard PortProtector Features | How to apply SafeGuard PortProtector policies for FISMA compliance |
|---|---|---|---|
| AC-3 (1) | Access Enforcement: The information system restricts access to privileged functions and security-relevant information to explicitly authorized personnel. | SafeGuard PortProtector prevents the use of unauthorized devices on network computers, and can prevent certain file types from being copied to storage media. Different policies can be applied to different users, so authorized personnel can get higher permissions. | In the Policies World, create a New Policy, and configure it as needed. To set file type control, click the File Control tab in security policies. |

| Requirement Number | Requirement Description | Relevant SafeGuard PortProtector Features | How to apply SafeGuard PortProtector policies for FISMA compliance |
|---|---|---|---|
| AC-18 (1) (2) | Wireless Access Restrictions: The organization uses authentication and encryption to protect wireless access and scans for unauthorized wireless access points. | SafeGuard PortProtector allows the organization to create policies that force the use of encrypted Wi-Fi channels for secure transfer of data. These policies can even be set to require a specific level of encryption (e.g., WPA).<br><br>In addition, SafeGuard PortProtector provides anti-bridging capabilities, preventing computers from connecting to wireless networks while connected to the organizational LAN. | Under port control, restrict Wi-Fi networks. Under Wi-Fi networks set a white list of approved Wi-Fi networks to WPA encrypted networks.<br><br>To restrict anti-bridging, set "Hybrid Network Bridging" to Block. |
| AC-19 | Access Control for Portable and Mobile Devices: The organization establishes usage restrictions and implementation guidance for portable and mobile devices; and authorizes, monitors, and controls device access to organizational information systems. | SafeGuard PortProtector provides the ability to control access to portable storage devices such as USB drives, PDAs, and mobile phones. The flexibility of SafeGuard PortProtector policies allows for a granularity of control that matches the organization's needs.<br><br>SafeGuard PortProtector also provides encryption for hard-disks and removable storage, | Configure SafeGuard PortProtector to control media and storage device use on desktops and laptops. The built-in FISMA policy provides explanations for these settings. |

| Requirement Number | Requirement Description | Relevant SafeGuard PortProtector Features | How to apply SafeGuard PortProtector policies for FISMA compliance |
|---|---|---|---|
| | | so unauthorized users cannot access secure data. | |
| AC-20 (1) | Use of External Information Systems: The organization prohibits authorized individuals from using an external information system to<br><br>access the information system or to process, store, or transmit organization-controlled information<br><br>except in specific, authorized cases. | SafeGuard PortProtector contains the option of restricting the organization's encrypted storage device from being used outside of the organization.<br><br>Using File Type Control, organizations can restrict the type of files that can be copied to/from external storage devices. | In security policies, under Media Encryption, make sure the "allow users to access devices on unprotected machines" option is not selected.<br><br>To set File Type Control, click the File Control tab in security policies and choose which files should be restricted. |
| AU-2 (1) (2) (3) | Auditable Events: The information system provides the capability to compile audit records from multiple components throughout the system, manage selection, and update them as needed. | Sophos products provide extensive and granular logging options, collected in several log types:<br><br>Client Logs<br><br>File Logs<br><br>Server Logs | Configure SafeGuard PortProtector to collect logs and send alerts according to your organization's policy. The built-in FISMA policy provides recommended pre-configured logging levels. |
| AU-3 (1) (2) | Content of Auditable Events: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events, and to expand and centrally manage events | SafeGuard PortProtector provides in-depth and granular logging and alerting options, both for security and administrative events. | For each action, set the Log and/or Alerts checkboxes for desired security actions. |

| Requirement Number | Requirement Description | Relevant SafeGuard PortProtector Features | How to apply SafeGuard PortProtector policies for FISMA compliance |
|---|---|---|---|
| | throughout the system. | | |
| AU-6 (1) (2) | Audit Monitoring, Analysis, and Reporting: The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting, and employs automated mechanisms to alert security personnel of inappropriate or unusual activities. | SafeGuard PortProtector provides alerts, which can be sent immediately and automatically to outside sources such as mail, event viewer, or SNMP.In addition to SafeGuard PortProtector built-in alerting and reporting options, SafeGuard PortProtector also provides integration with SIEM systems, ensuring that security administrators can keep track of security events regardless of their chosen system. | In the Administration dialog, configure Alert Destinations.<br><br>In security policies, under Alerts, choose the desired Destinations. |
| AU-8 (1) | Time Stamps: The information system provides time stamps for use in audit record generation, and allows synchronization with internal information system clocks. | SafeGuard PortProtector logs contain the time stamp of both the endpoint where the event originated from, as well as that of the management server. | To synchronize the time stamps, set both the server machine and endpoint machines to sync with network time servers. These settings are usually configured by default by the directory services. |

<table>
<tr><th>Requirement Number</th><th>Requirement Description</th><th>Relevant SafeGuard PortProtector Features</th><th>How to apply SafeGuard PortProtector policies for FISMA compliance</th></tr>
<tr><td>CM-2 (1) (2)</td><td>Baseline Configuration: The organization develops, documents, and maintains a current baseline configuration and employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.</td><td rowspan="3">SafeGuard PortProtector security policies contain extensive and granular definitions for restricting the use of ports, storage and non-storage devices, and enforcing restrictions.<br><br>SafeGuard PortProtector includes a built-in policy server, which securely updates endpoint policies (either immediately from the server, or at periodic intervals).<br><br>The server manages and displays the protection status, details, and log information of each endpoint.<br><br>For CM-5, add info about role-based management and partitioning</td><td rowspan="3">In the Clients World, display network computers (search by name or by browsing directory tree), and view status and details of each computer.<br><br>In security policies, configure automatic log retrieval and policy update interval either globally or per each policy separately.</td></tr>
<tr><td>CM-5 (1)</td><td>Access Restrictions for Change: The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.</td></tr>
<tr><td>CM-6 (1)</td><td>Configuration Settings: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.</td></tr>
</table>

| Requirement Number | Requirement Description | Relevant SafeGuard PortProtector Features | How to apply SafeGuard PortProtector policies for FISMA compliance |
|---|---|---|---|
| CM-7 (1) | Least Functionality: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the functions and ports. | SafeGuard PortProtector security policies can be set to completely lock down organizational endpoint and allow only necessary permissions to approved users. Logs can be set to detect any unauthorized usage attempt. See also item MP-2. | In security policies, define which devices are allowed and blocked, or use the built-in FISMA policy with recommended, pre-configured permissions.<br>Policies can be configured either for users or for computers, providing a high level of granularity of configuration. |
| CM-8 (1) (2) | Information System Component Inventory: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. | SafeGuard PortProtector maintains and displays a list of all computers in the organization and their current protection status. By using SafeGuard PortAuditor, it is possible to view all devices being used or previously connected to the network computers. | Open the Clients World to view network computers and filter them by status.<br>Use SafeGuard PortAuditor to view all devices currently and previously connected to network computers. |
| CP-7 (1) (2) (3) (4) | Alternate Processing Site: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions. | SafeGuard PortProtector Management Server includes cluster support, for full redundancy and load-balancing. | When installing additional management servers, choose the "Cluster" installation option. |

| **Requirement Number** | **Requirement Description** | **Relevant SafeGuard PortProtector Features** | **How to apply SafeGuard PortProtector policies for FISMA compliance** |
|---|---|---|---|
| CP-9 (1) (2) (3) (4) | Information System Backup: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system. | SafeGuard PortProtector provides measures for creating encrypted backups of both the system configuration, and the security logs database. | In the Administration window, select *Maintenance* and choose backup options and schedule. |
| CP-10 (1) | Information System Recovery and Reconstitution: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. | SafeGuard PortProtectors provides an easy mechanism for recovering servers using backup keys. | In the SafeGuard PortProtector Install Wizard, choose the *Restore* option to import pre-existing backup keys and configuration. |
| IA-3 | Device Identification and Authentication: The information system identifies and authenticates specific devices before establishing a connection. | SafeGuard PortProtector security policies can restrict access to storage and non-storage devices, and create exemptions based on vendor and product ID (for models), or serial number for specific devices, and log all access attempts according to VID, PID, serial number, user, and machine. | Set the security action for the device type to *restrict*, and select *white list* to add exemptions by VID, PID, or serial number. |
| IR-4 (1) | Incident Handling: The organization employs automated mechanisms to support the incident handling process. | By using alerts, it is possible to automatically receive real-time incident information notification. | Open the Administration dialog, click *Logs & Alerts*, and create new alert destinations. Set security policies to export alerts to them. |
| IR-5 (1) | Incident Monitoring: The organization employs automated mechanisms to assist in the tracking of security incidents and in | Alerts can be | |

| Requirement Number | Requirement Description | Relevant SafeGuard PortProtector Features | How to apply SafeGuard PortProtector policies for FISMA compliance |
|---|---|---|---|
| | the collection and analysis of incident information. | exported to email, event viewer, syslog, and external systems, via SNMP or executable scripts. | |
| IR-6 (1) | Incident Reporting: The organization employs automated mechanisms to assist in the reporting of security incidents. | | |
| MA-5 | Maintenance Personnel: The organization allows only authorized personnel to perform maintenance on the information system. | SafeGuard PortProtector enables role-based management and domain partitioning. It is possible to define different administrative permissions for different system functions and only for specific parts of the network. | Open the Administration window. In General, under *Users Management* click the *Role Based (Advanced)* option, and define roles and domain partitions as needed. |
| MP-2 (1) | Media Access: The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. | SafeGuard PortProtector security policies provide granular policies to set in-depth permissions for device access and allow only necessary permissions. Logs can be set to detect any unauthorized usage attempt. | In security policies, define which devices are allowed and blocked, or use the built-in FISMA policy with recommended, pre-configured permissions. |

| Requirement Number | Requirement Description | Relevant SafeGuard PortProtector Features | How to apply SafeGuard PortProtector policies for FISMA compliance |
|---|---|---|---|
| MP-5 (1) (2) | Media Transport: The organization protects digital and non-digital media during transport outside of controlled areas and documents, where appropriate, activities associated with the transport of the media. | SafeGuard PortProtector provides built-in media encryption capabilities based on AES 256-bit encryption. Permissions can be set to limit use of encrypted devices to organizational computers only, or allow use outside of the network (offline) with password. | In security policies, under *Storage Control*, define which devices should be encrypted, or use the built-in FISMA policy with recommended, pre-configured settings, which by default encrypts all storage devices. |
| SI-4 (2) (4) (5) | Information System Monitoring Tools and Techniques: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. | SafeGuard PortProtector includes extensive logging, alerting, and shadowing capabilities, which notify administrators of any security incidents and the content of data copied to removable storage devices. | To set logging and alert levels for administrative events, open the Administration window and select *Logs & Alerts*.<br><br>To set logging for security incidents, modify both security policies and *Global Policy Settings* as needed. |
| SI-5 (1) | Security Alerts and Advisories: The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed. | SafeGuard PortProtector security policies include a large number of customizable end-user messages, which alerts the user of administrative changes (such as policy update), or security incidents (such as a device being blocked). Administrators can modify messages according to their | In security policies, click the *End User Messages* tab, and modify end-user messages as needed. |

| **Requirement Number** | **Requirement Description** | **Relevant SafeGuard PortProtector Features** | **How to apply SafeGuard PortProtector policies for FISMA compliance** |
|---|---|---|---|
| | | needs. | |
| SI-7 (1) (2) | Software and Information Integrity: The information system detects and protects against unauthorized changes to software and information and employs automated tools that provide notification to appropriate individuals upon discovering discrepancies. | SafeGuard PortProtector includes redundant, multi-tiered anti-tampering measures, which prevent users from circumventing security policy. When such attempts are detected, the machine is automatically locked down, and logs and alerts are generated to notify security administrators. | SafeGuard PortProtector anti-tampering measures are enabled by default, and no administrator action is required.<br>In addition, SafeGuard PortProtector encrypts all system logs and configuration files, and system communications, so they cannot be read or modified by unauthorized users. |